FATF

Mutual Evaluation of Belgium

Anti-money laundering and countering the financing of terrorism and proliferation financing measures

December 2025

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

How to read this mutual evaluation report

The Financial Action Task Force (FATF) has revised its assessment methodology to place an even greater focus on effectiveness, to ensure that countries are implementing and making use of the laws, regulations and policies that are being passed, as well as a greater emphasis on the major risks and context. This round of mutual evaluations is operating on a six-year cycle, significantly shorter than earlier rounds, and includes time-bound Key Recommended Actions roadmaps for countries that need to improve in key areas.

Effectiveness has been assessed according to the 11 immediate outcomes that an effective anti-money laundering/countering the financing of terrorism/countering proliferation financing (AML/CFT/CPF) framework should be able to deliver. The extent to which a country is taking effective action in this area is reflected in ratings that range from low to high level of effectiveness (see chapters 1 – 11).

Technical compliance has been re-assessed in line with the FATF Recommendations where: (i) the country has made legal, regulatory or operational framework changes since its last mutual evaluation or follow-up report with technical compliance re-ratings and (ii) there has been a change in the FATF Standards for which the country has not previously been assessed. Where technical compliance has been reassessed, the relevant section is clearly indicated in the Technical Compliance Annex. Where a Recommendation has not been re-assessed, the previous assessment is included under a grey heading (see Technical Compliance Annex – Annex A).

A glossary of key terms is available at the end of the report.

Citing reference:

FATF (2025), *Mutual Evaluation Report of Belgium*, FATF, Paris, www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/mer-belgium-2025.html

Table of contents

Executive summary

1. This report provides a summary of the anti-money laundering and counter-terrorist financing (AML/CFT) measures in place in Belgium as at the date of the on-site visit (27 January to 14 February 2025). This report analyses the level of compliance with the FATF 40 Recommendations and the effectiveness of Belgium's AML/CFT system, and provides recommendations on how this system could be improved.

Key Findings

a) Belgium applies an AML/CFT system that is technically largely aligned with the FATF Recommendations, following legislative and regulatory reforms carried out since the 2015 Mutual Evaluation Report (MER). New measures are beginning to show results, but significant improvements are still needed to improve effectiveness.

b) The persistent lack of resources allocated to AML in Belgium has an impact on the effectiveness of the law enforcement approach implemented by the competent authorities. The resources available to the authorities to investigate and prosecute ML and predicate offences are not commensurate with the challenges Belgium faces. This recommendation was already made in the 2015 MER, but no corrective measures have been taken to address it. This lack of resources affecting the police and judicial authorities prevents Belgium from systematically and as a matter of priority tackling organised crime networks with international ramifications operating in the country, and hinders the country's ability to deprive criminals of the proceeds generated by ML activities and predicate offences.

c) Belgium is facing a confirmed and growing risk of virtual assets (VA) being used for ML and TF purposes. The Belgian authorities are making progress in their knowledge and understanding of the ML/TF risks and mechanisms associated with VAs, but expertise should be deepened and supported by appropriate tools, including in cooperation with the private sector, in order to better understand the risks associated with this sector. Belgium should also prioritise the definition of a strategic approach in order to better anticipate and manage the ML/TF risks associated with VAs. Finally, Belgium should adopt as soon as possible a legislative or regulatory framework designating the competent authority for the licensing and supervision of VA service providers (VASPs), in accordance with the requirements of the European regulation applicable since 31 December 2024 ("MiCA" Regulation).

d) Belgium has a generally satisfactory understanding of its ML/TF risks, based on national risk analyses that are regularly updated and developed in cooperation between the competent authorities. These risk analyses highlight the growing prevalence of large-scale criminal schemes involving, in addition to the aforementioned VAs, drug and cash trafficking, professional money launderers, and organised crime networks, with growing polycriminal activities and increasing links between ML and TF. However, Belgium's response is not commensurate with the level and nature of the risks identified. It should adopt a strategic approach, based on clear priorities and backed by adequate resources, in order to comprehensively tackle the major crime patterns developing in the country. It should prioritise underground financial channels, including through the use of cash and illicit money transfers and VA activities, in order to stem the sources of the main criminal activities leading to ML and TF.

e) Belgium has adopted transparency measures to address the high risk of ML/TF associated with the abuse of legal persons and legal arrangements in the country, particularly in relation to offsetting mechanisms. The creation of a register of beneficial owners in September 2018 (UBO register) has enabled Belgium to expand its multi-pronged approach to accessing information on beneficial owners. This register is a useful tool for accessing the necessary data, and Belgium should capitalise on its functionalities by ensuring that effective verification measures are taken to guarantee that the data already recorded, and to be recorded in the future, is accurate and up to date. The reform of the Belgian Companies and Associations Code in 2019 also led to a major transformation of the landscape of legal persons in Belgium, in particular by facilitating their creation. This has resulted in an increase in shell and dormant entities, calling for the adoption of appropriate mitigating measures.

f) Belgium adjusted its response to terrorism following the attacks in 2015/2016. It implements an operational CFT strategy that allows it to deal with all targets likely to be involved in TF activities. However, formal integration of TF is necessary into the counter-terrorism strategy, and also the operational handling of TF cases. This would allow for a more coherent, forward-looking and responsive approach to TF risks – one that can anticipate and adapt to changes in the country's TF risk profile.

g) Belgium should strengthen its AML/CFT framework by applying rigorous dissuasive policy to sanction both reporting entities that fail to implement AMLFT preventive measures and criminals convicted of ML and TF offences.

Ratings for effectiveness and technical compliance

	Effectiveness		Technical Compliance	
Risk mitigation through policy, co-ordination and co-operation				
Assessment of risk, coordination and policy setting	**IO.1**	Moderate	**R.1**	Largely compliant
			R.2	Partially compliant
International co-operation	**IO.2**	Moderate	**R.36**	Compliant
			R.37	Largely compliant
			R.38	Largely compliant
			R.39	Largely compliant
			R.40	Largely compliant
Cross-cutting requirements			**R.33**	Largely compliant
Prevention, detection & reporting of illicit funds across sectors				
Financial sector and virtual asset supervision and preventive measures	**IO.3**	Moderate	**R.9**	Compliant
			R.10	Compliant
			R.11	Largely compliant
			R.12	Compliant
			R.13	Partially compliant
			R.14	Compliant
			R.15	Non-compliant
			R.16	Largely compliant
			R.17	Largely compliant
			R.18	Largely compliant
			R.19	Compliant
			R.20	Largely compliant
			R.21	Compliant
			R.26	Compliant
			R.27	Compliant
Non-financial sector supervision and preventive measures	**IO.4**	Moderate	**R.22**	Largely compliant
			R.23	Largely compliant
			R.28	Largely compliant
Transparency and beneficial ownership	**IO.5**	Moderate	**R.24**	Partially compliant
			R.25	Largely compliant
Cross-cutting requirements			**R.34**	Largely compliant
			R.35	Compliant
Detection and disruption of threats, sanctions & deprivation of illicit funds				
Financial intelligence	**IO.6**	Substantial	**R.29**	Largely compliant
Money laundering investigations and prosecutions	**IO.7**	Moderate	**R.3**	Largely compliant
Asset recovery	**IO.8**	Moderate	**R.4**	Largely compliant
			R.32	Partially compliant
Terrorist financing investigations and prosecutions	**IO.9**	Substantial	**R.5**	Compliant
Terrorist financing preventive measures and financial sanctions	**IO.10**	Moderate	**R.6**	Partially compliant
			R.8	Partially compliant
Proliferation financing financial sanctions	**IO.11**	Moderate	**R.7**	Largely compliant
Cross-cutting requirements			**R.30**	Compliant
			R.31	Compliant

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness. Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non-compliant. While the technical compliance findings can be relevant across the effectiveness immediate outcomes (for example, R.1 or R.40), the table above illustrates the main technical compliance findings specific to each effectiveness immediate outcome and cross-cutting requirements for each of the intermediate outcomes. For more detail on the relevant technical compliance requirements relevant to each effectiveness immediate outcome, see the relevant paragraph at the beginning of each chapter. See also paragraphs 53 and 54 of the FATF 2022 Methodology for links between effectiveness and technical compliance ratings.

Risks and general situation

2. The structural, institutional and geographical characteristics of Belgium expose the country to significant financial and non-financial flows, which may be conducive to the development of criminal phenomena. The port of Antwerp is a point of entry and an international logistics platform for legal and illegal goods and merchandise. Furthermore, Belgium has a high level of tax and social charges within the EU, which tends to encourage fraud.

3. For ML, Belgium is mainly exposed to criminal threats associated with cash trafficking, drug trafficking, social and tax fraud, other types of fraud and organised crime. Corruption also appears to be an increasingly significant ML threat. Belgium's ML environment is marked by a high degree of interconnection between criminal activities, which increases the opacity of the schemes and modus operandi leading to ML activities and the involvement of professional launderers. Criminals tend to invest in sectors and activities not covered by the scope of the AML regime, which increases the complexity of ML networks and makes them less visible to the authorities. One of the main vectors of ML in the country is the offsetting technique, which combines the massive use of cash with polycriminal activities such as social fraud, abuse of legal structures and drug trafficking.

4. Regarding the terrorist financing (TF) threat, the main threat in Belgium relates to ex-foreign terrorist fighters and radicalised individuals, via micro-financing involving new payment methods and small cash transactions, mainly of legal origin.

5. In addition, the national risk analyses carried out by Belgium and a number of recent cases reveal the growing use of virtual assets by criminals in ML and TF typologies.

6. Belgium implements an effective AML/CFT system for financial intelligence, with the FIU (CTIF) as the central body for collecting, enriching, analysing and disseminating information. TF investigations and prosecutions are also conducted effectively, supported by an operational counter-terrorism and TF approach developed after the 2015/2016 attacks, to improve coordination and information flows among competent authorities. Since the 2015 MER, Belgium has taken further AML/CFT measures, including broadening the scope of AML/CFT reporting entities in 2017, introducing a beneficial ownership register in 2018, initiatives to overcome obstacles to international cooperation between judicial authorities, and an AML Action Plan in 2024. All these initiatives are beginning to bear fruit, but major improvements are still required to increase the effectiveness of the Belgian system vis-à-vis the assessment and understanding of ML/FT risks, international cooperation, supervision and the implementation of preventive measures by financial and non-financial institutions and VASPs, the transparency of legal persons and legal arrangements, the investigation and prosecution of ML, confiscation of the proceeds of crime, and the application of targeted financial sanctions (TFS) in relation to TF and proliferation financing (PF), as well as the prevention of misuse of the non-profit sector for TF purposes. In particular, the lack of resources to enable the police and judicial authorities to carry out their investigations and prosecutions of ML calls for urgent action on the part of Belgium.

7. In terms of technical compliance, Belgium's AML/CFT legal and institutional framework is largely in line with the requirements of the FATF Recommendations. Since the 2015 MER, Belgium has carried out the necessary legislative and regulatory reforms, such as the implementation of an operational framework in 2016 for the national freezing mechanism in TF matters, the introduction of the AML Law in 2017 for the transposition of the fourth and fifth European AML Directives, the provision of access for all competent authorities to the centralised register of financial accounts and contracts held by legal persons with financial institutions in 2018, and the adoption of national provisions for the implementation of the TFS without delay in 2019. However, shortcomings are still apparent in certain areas, such as the application of the new European rules governing VASPs, the transparency rules applicable to legal persons, the oversight of cross-

border movements of funds, stronger measures in relation to correspondent banking and the regime applicable to non-profit organisations at risk of TF abuse.

Risk assessment, coordination and definition of policies (Chapter 1 - IO.1; R.1, R.2, R.33 and R.34)

8. Belgium has a satisfactory understanding of ML/TF risks, which are regularly assessed by the competent authorities on a collaborative basis. The authorities are improving their knowledge and understanding of the ML/TF risks associated with VAs, but their expertise remains inadequate given the confirmed and growing risks of VA-based ML and TF. Belgium should therefore prioritise measures designed to provide greater control over these mechanisms. Furthermore, a significant proportion of criminal activity takes place outside the formal, regulated AML/CFT sector, including through cash trafficking, and Belgium should adopt a strategic approach to improve the detection and supervision of these alternative financial circuits.

9. Belgium adopted an action plan in 2024 to guide its national AML policy. In general, it contains necessary measures but does not reflect a strategic, long-term approach to stemming the sources of the main criminal activities in Belgium and tackling the links between ML and organised crime. Belgium should develop an AML/CFT strategy based on the country's strategic priorities, targeting the major crime phenomena identified in national risk analyses.

10. The majority of Belgian authorities conduct sectoral risk analyses, which contribute to their overall understanding of ML/TF risks and provide a good basis for developing mitigation measures and prioritising activities. These sectoral and national analyses should better inform each other in order to further improve the knowledge of ML/TF risks and typologies. Belgium also provides for exemptions from the AML/CFT regime (games of chance, certain activities of company service providers) which might no longer be justified by a low level of risk in the light of developments in the sectors concerned and which should be reassessed.

11. The understanding of TF risks is sound and could be further enhanced by a more granular approach and a more precise contextualisation of the threats identified in the country. This would facilitate the anticipation of changes in risk and the adaptation of responses, even if the operational strategy adopted currently allows action to be taken in relation to all the identified targets.

12. Institutional and operational cooperation for AML purposes is generally effective but it could be improved in the TF field by associating TF experts more closely with terrorism experts.

International cooperation (Chapter 2; IO.2 ; R.36–40)

13. International cooperation is a central aspect of AML/CFT activities in Belgium due to the country's characteristics, and a substantial proportion of the country's AML/CFT circuits have foreign components. Belgium has not comprehensively mapped the type of cases for which it has received requests or contacted its foreign counterparts, and the result(s) obtained, which makes it difficult to assess the alignment of its international cooperation activities with the country's ML/TF risk profile and the impact of requests on its international cooperation. This especially applies to mutual assistance for asset recovery, a field in which international cooperation should be a high priority for the country.

14. Nevertheless, Belgium has demonstrated through some cases that international cooperation has helped to solve complex ML cases, including the dismantling of networks with ramifications abroad in offsetting schemes. Belgium has also engaged in numerous collaborations with foreign partners, through diplomatic channels and bilaterally between judicial authorities, in order to facilitate and accelerate

international cooperation. Some of these initiatives have already produced results and should be accelerated to maximise their full impact and ensure their long-term implementation.

15. However, in the absence of comprehensive data for all public prosecutors' offices in ML cases, it is unclear whether international cooperation measures are being implemented systematically, particularly for cases managed by district public prosecutors' offices outside Brussels. In addition, the general lack of resources for ML investigations and prosecutions (see IO.7) affects Belgium's ability to implement the resources required to systematically pursue the international component of ML cases.

16. The Belgian authorities make regular and fairly systematic use of informal cooperation to support their AML/CFT activities and provide high-quality support according to the feedback received from Global Network members.

Financial sector and virtual asset supervision and preventive measures (Chapter 3; IO.3 ; R.9-21, R.26-27, R.34 and R.35)

17. Since the entry in force of the MiCA regulation (31 December 2024),[1] no authority has been designated in Belgium to licence and supervise VASPs, leaving this very high-risk sector without adequate oversight. At the time of the on-site visit, no VASP was registered or licenced in Belgium.

18. The main supervisory authorities for financial institutions – the BNB and the FSMA – effectively supervise market access, but the detection of illicit activities remains limited, particularly for hawala transfers and virtual assets.

19. Supervisory authorities and the highest-risk FIs, including credit institutions (CIs), have a generally satisfactory understanding of ML/TF risks. This understanding is reflected in supervision that is generally adapted to the levels of risk identified, based on an appropriate risk-based approach. BNB and FSMA have a wide range of off-site and on-site supervisory actions at their disposal. On-site inspections are generally thorough and of good quality. The remote supervision of the BNB, which oversees the FIs with the highest exposure to ML/TF risks, is generally appropriate. On-site inspections can take place well after they are scheduled – up to a year later – and can sometimes extend over very long periods, which can reduce their impact and effectiveness. They are insufficient for electronic money institutions and, to a lesser extent, payment institutions.

20. FSMA's remote inspections, which accounts for the bulk of its controls, focus on formal compliance. Their impact could be reinforced by integrating more operational data into some of these controls. In addition, their frequency should be reviewed to prevent certain higher-risk entities (managers of small alternative investment funds and lenders) from escaping substantial scrutiny for long periods of time.

21. Furthermore, the very limited use of administrative sanctions by the BNB and the FSMA, combined with the almost non-existent or anonymous publication of decisions, considerably weakens the dissuasive effect and educational aspects of the repressive system. The effective use of these sanctions should be strengthened by adapting human resources and, if necessary, the applicable legal framework.

22. FIs – especially CIs and currency exchange offices (bureaux de change)– apply generally satisfactory preventive measures. They are applied more inconsistently by the other FIs supervised by the FSMA. While STRs are increasing overall, particularly among CIs, significant delays in reporting time remain.

[1] Regulation (EU) 2023/1114 on markets in crypto-assets

Non-financial sector supervision and preventive measures (Chapter 4; IO.4 ; R.9-21, R.26-27, R.34 and R.35)

23. All professions are subject to basic verification procedures, but more advanced requirements (training, transparency of beneficial owners) and post-registration controls remain limited.

24. Some supervisory authorities – particularly in the diamond sector, which is most at risk of ML/TF – have a good understanding of ML risks. However, the understanding of TF risks is generally low throughout all authorities and reporting entities. Sectoral analyses often lack depth, merely repeating elements of the national analysis without making any specific inputs.

25. Supervision is fragmented and uneven. SPF Economy, which is responsible for the sectors most at risk (estate agents, diamond dealers, business centres), is understaffed and carries out a limited number of inspections, despite high non-compliance rates. Some self-regulated professions are better supervised, but the scope of these controls often remain limited. Competent authorities' human and technical resources need to be strengthened to ensure a targeted and effective supervision, particularly for the sectors most at risk, such as diamond dealers.

26. Sanctions are rare and often anonymous, which significantly reduces their dissuasive effect. More effective, proportionate and visible use of sanctions should be ensured, particularly in sectors where guidance still largely prevails over supervision (notaries, lawyers, business centres). For diamond dealers, the absence of graduated sanctions leads to excessive measures (such as licence suspension), which undermine the proportionality of the system. The small number of inspections also limits the assessment of their actual impact on compliance. The scope of awareness-raising and training initiatives should be broadened and better targeted, in view of the persistent high non-compliance rates.

Transparency and beneficial ownership (Chapter 5 – IO.5; R.24 and R.25)

27. Belgium has a general understanding of the ML/TF risks to which legal persons and legal arrangements are exposed. This understanding is sometimes uneven and should be further developed taking into account Belgium's specific context of polycriminal activities, where the abuse of legal persons and legal arrangements has been identified as a major ML risk, and a lesser TF risk.

28. Belgium adopts a multi-pronged approach to collect basic and beneficial ownership information, based on different interconnected registers and information held by reporting entities and the legal entities themselves. The creation of the beneficial ownership register (UBO register) in September 2018 is an important tool to strengthen the transparency framework, and registration rates are very high (around 98%). However, the basic information registers (Banque-Carrefour des Entreprises and the UBO register) do not provide accurate, reliable and up-to-date information due to major shortcomings in the verification of information recorded. Belgium should apply rigorous verification mechanisms to enable registers to achieve their full potential and provide the competent authorities with access to reliable information.

29. Belgium implements measures to mitigate the risks of abuse of legal persons and legal arrangements that only moderately address the identified risks. The competent authorities are steadily striking off and dissolving inactive entities to counter the use of shell entities and shell companies, whose creation was facilitated by the reform of the Belgian Companies and Associations Code (CSA) in 2019. These measures should be accelerated. The targeted checks on existing data launched by the UBO register in September 2024 should also be intensified. The stock of notifications of differences received, particularly from FIs, should be prioritised. Furthermore, Belgium should adopt the necessary measures to ensure greater transparency in the use of nominee directors and shareholders, and thus of straw-men, which are an important source of vulnerability for the country.

30. Belgium does not authorise the creation of trusts or similar legal arrangements. However, foreign legal arrangements may be administered by a Belgian resident or hold property or rights in Belgium. Belgium is not in a position to ensure that foreign legal arrangements with links to Belgium actually comply with their transparency obligations. The information available to the tax authorities should be used more actively to help increase the transparency of legal persons and arrangements operating in Belgium. In addition, the understanding of the risks associated with foreign legal persons and arrangements with sufficient links to Belgium should be deepened.

Financial intelligence (Chapter 6 - IO.6; R.29-32)

31. The CTIF plays a key role in producing financial intelligence for countering ML/TF, at both operational and strategic levels, and largely meets the operational needs of competent authorities. It is regularly asked to enrich investigations, drawing on a large volume of STRs and other relevant information and its extensive access to many administrative and financial databases. Cooperation and the sharing of financial information and intelligence between the competent authorities is close, fluid and constructive. The dissemination of CTIF's typological analyses should be broadened to strengthen the strategic support to competent authorities and better feed into the identification of risks and the detection of emerging threats.

32. However, the IT tools currently available to the CTIF are insufficient to process and exploit the growing and increasingly complex volume of information, which limits the scope of its analyses. The recent roll-out (October 2024) of the goAML platform aims to address some of these technical limitations (lack of segmentation, delay tracking, etc.), but further improvements are still required to ensure optimum use of financial intelligence and to strengthen strategic analysis capacities.

33. The use of financial intelligence by competent authorities for ML purposes is insufficient. In particular, the information held by Customs and tax authorities, although essential in the Belgian context marked by the scale of international cash trafficking and the prevalence of social and tax fraud, remains under-exploited by the law enforcement authorities. Targeted reinforcement of the skills of judicial authorities, as well as the development of tools adapted to the processing of financial intelligence, are necessary to increase its effective integration into ML investigations.

Money laundering investigations and prosecutions (Chapter 7 – IO.7; R.3, R.30 and R.31)

34. Belgium identifies ML cases mainly from police sources. Data exploited from the SKY ECC case has for example been used, since 2021, to launch and enhance investigations into ML and organised drug trafficking – offences to which Belgium is highly exposed. However, the lack of a strategic and targeted approach to detecting ML and the under-utilisation of the financial intelligence and information emanating from CTIF (see above) do not allow Belgium to adopt an effective enforcement approach to countering the main criminal activities generating ML that the country faces: organised crime, polycriminal professional ML, cash trafficking, crime associated with the diamond sector, and financial activities via illicit mechanisms, as well as the growing use of VAs. Belgium should implement a targeted ML detection strategy to proactively tackle the criminal networks operating in the country.

35. Belgium has demonstrated its ability to prosecute large-scale ML cases, showing that it has the operational potential to handle such cases. It has a legal and jurisprudential framework that should facilitate the proof of ML by not requiring the establishment of a link between the predicate offence and ML. However, the characteristics of the cases generally prosecuted are not fully in line with the country's risk profile, and complex ML cases account for only a limited proportion of the cases handled. Belgium does not prioritise tackling criminal networks, although some complex cases involving criminal organisations

have resulted in convictions. It should apply a crime policy that prioritises the dismantling of criminal networks active in Belgium and the forms of crime prevalent in the country for ML.

36. Belgium does not have the human and technological resources needed to effectively counter the large-scale polycriminal ML phenomena to which it is exposed. This is reflected notably by the prioritisation of ML cases based on the profitability of opening an investigation, which does not orient investigations and prosecutions towards complex ML cases, but rather towards those for which assets are immediately and easily available. Generally speaking, investigations are limited to the predicate facts, without sufficiently in-depth financial investigations being carried out. The Federal Police Criminal Investigation Department (Police Judiciaire Fédérale – PJF) has issued internal directives to strengthen the financial component of investigations, but their effective implementation would require the allocation of adequate human and technological resources. As previously recommended in the 2015 MER, Belgium should provide the law enforcement and judicial authorities with the human, financial and technological resources needed to tackle the root causes of the criminal activities affecting the country.

37. Belgium should also ensure that effective and dissuasive sanctions are imposed on criminals convicted of ML offences and restrict the use of the transaction procedure in ML cases, which must not replace criminal prosecution and must include guarantees of transparency and public disclosure of the agreements reached.

Confiscation (Chapter 8 – IO.8; R.1, R.4 and R.32)

38. Belgium only deprives criminals of illegally obtained assets to a limited extent. It has a solid legal framework and prioritises the recovery of criminal assets to a certain extent. However, this prioritisation is not accompanied by sufficient resources and tools to be implemented effectively. Belgium does not carry out sufficiently in-depth financial investigations into ML (see IO.7). In addition, the lack of police resources impacts the authorities' ability to identify and appropriately confiscate criminal assets derived from ML and the predicate offences. Lastly, the enforcement of confiscation measures ordered in the absence of prior seizure encounters major difficulties and the actual recovery rate is low.

39. Belgium should provide the competent authorities (investigating authorities, prosecuting authorities and the Central Office for Seizures and Confiscations with the resources they need to carry out in-depth financial investigations and criminal enforcement investigations more systematically and thus obtain results commensurate with the risks to which it is exposed.

40. Belgium has identified the movement of cash linked to international trafficking in cash and bearer negotiable instruments (BNI) as a major predicate crime for ML. However, the confiscation of cash and BNIs associated with illicit cross-border cash transportation is only used to a limited extent in the identification and tracing of potential ML-related assets. The lack of a strategic approach to monitoring cash movements, particularly within the EU and linked to transit through the port of Antwerp, prevents Belgium from targeting the main sources of these flows and from confiscating assets commensurate with the risks to which Belgium is exposed. Belgium should implement a strategic approach, backed by the necessary resources, to target customs controls of accompanied and unaccompanied movements of cash and BNIs more effectively and to use information from customs and police authorities on cross-border cash transportation more strategically, with a view to bringing confiscations to a level commensurate with the identified risks of cash trafficking to which Belgium is exposed.

Terrorist financing investigations and prosecutions (Chapter 9 – IO.9; R.5, R.30, R.31 and R.39)

41. Overall, Belgium has a solid and well-structured system for detecting and dealing with FT cases, based on an integrated operational approach covering the fight against terrorism and its financing. This response, strengthened after the 2015/2016 attacks, is supported by inter-institutional coordination platforms ("Joint Intelligence Center" – JIC and "Joint Decision Center" – JDC), deployed nationwide since 2023. This approach ensures the rapid detection and consistent processing of TF cases, in line with the country's TF risk profile. The operational capabilities and resources of the Federal Public Prosecutor's Office are adapted to current needs. Available information indicates that the JIC/JDC have handled all TF investigations. However, the lack of consolidated data on TF cases identified or handled via the JIC/JDC makes it difficult to evaluate their real contribution. Belgium should implement a formalised monitoring and feedback mechanism for TF cases handled by the JIC/JDC platforms, in order to strengthen the sharing of lessons learned between departments and disseminate best practices more widely.

42. In addition, the authorities do not currently appear to be sufficiently equipped to adapt their TF approach rapidly to new methods of financing, particularly via VAs or informal channels, the detection of which remains limited. A more proactive response, including adapting to emerging technologies and bypassing traditional financial circuits, is required to maintain the effectiveness of the system.

43. The sanctions applied to TF cases are generally consistent, combining prison sentences, partial suspended sentences and probationary follow-up. In the majority of cases, they appear to be dissuasive. However, the use of alternative mechanisms to prosecution may raise questions when applied to family transfers – even small amounts – in a TF context, in view of the objectives of prevention and deterrence.

Terrorist financing preventive measures and financial sanctions (Chapter 10 – IO.10; R.1, R.4, R.6 and R.8)

44. Belgium amended its legal framework in 2019 to enable the UN designations to be applied without delay and has put in place an inter-institutional framework to identify the targets to be designated for TF. However, it does not play an active role in proposing designations for inclusion on UN sanctions lists. Since the attacks of 2015/2016, Belgium has favoured the application of national measures for the designation and freezing of TF assets. The criterion relating to the existence of criminal proceedings for a designation should be removed to comply with FATF requirements and enable persons and entities to be targeted more actively.

45. Only certain financial institutions (FIs) have implemented freezing measures in relation to designated persons and entities. The amount of frozen assets is broadly consistent with the country's TF risk profile. The situation is less satisfactory for non-financial institutions, which have a limited understanding of their TFS obligations in relation to TF. Furthermore, their supervisory authorities also have a limited understanding of TFS mechanisms and do not monitor their implementation sufficiently, with the exception of SPF Economy, which oversees the diamond sector in particular. Belgium should take the necessary steps to improve the understanding of the obligations and the application of appropriate supervision to ensure the effective implementation of TFS for TF.

46. The Belgian authorities have a general understanding of the NPO sector and have conducted a specific risk assessment. However, this assessment does not make it possible to identify in an exhaustive and up-to-date manner the entities most exposed to TF risks, which limits the authorities' ability to target their actions (see R.8). In the absence of precise data on unregistered NPOs or those operating in sensitive areas without public funding, detection relies heavily on intelligence services or reports, rather than on a structured strategy based on objective criteria.

47. The controls currently in place – tax, accounting or related to the granting of public subsidies – are not tailored to the TF risk and do not specifically target non-subsidised NPOs or those operating in sensitive areas without accreditation. Furthermore, the requirements in place for some NPOs are cumbersome yet ineffective in preventing abuses for TF purposes. More targeted mitigation measures should be developed, accompanied by appropriate support for vulnerable entities, to ensure a proportionate approach better aligned with the identified risk profiles.

48. In addition, the lack of a dedicated structure for coordination between the various authorities with responsibilities for NPOs limits the overall vision and responsiveness of the system. Awareness-raising initiatives in the NPO sector remain ad hoc, poorly targeted, and do not yet include the profiles of the most at-risk NPOs. The provision of more targeted support would be important lever for improving prevention in this sector.

Proliferation financing financial sanctions (Chapter 11 – IO.11; R. 7)

49. Belgium has a legislative framework based mainly on European regulations to implement the Resolutions applicable to the Democratic People's Republic of Korea (DPRK). The implementation of TFS is currently the only measure in place in Belgium specifically targeting PF. The freezing measures implemented by FIs, although recent and limited, appear to be consistent with Belgium's PF risk level.

50. Belgium conducted its first national PF risk analysis in 2023, in which the identification, assessment and understanding of the risks of non-compliance, non-application and circumvention of PF sanctions related to the DPRK were not sufficiently assessed. Belgium should deepen its understanding of these risks and strengthen operational cooperation between the authorities holding information on the risks and technological developments associated with proliferation by the DPRK, in order to ensure that the measures in place are sufficient to mitigate identified risks. Moreover, the reporting entities' understanding of PF TFS is limited to identifying potential cases of violation and non-implementation of TFS. It does not extend to the identification of more sophisticated ways of circumventing PF TFS, which potentially impacts their ability to freeze property and assets. Risk indicators should be developed and applied to enable the identification of complex patterns of circumvention of PF TFS relating to the DPRK.

Roadmap of key recommended actions (KRAs)

Belgium underwent a Mutual Evaluation of its anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place during its on-site visit to the country from 27 January to 14 February 2025. This evaluation was based on the 2012 FATF Recommendations (as updated) and was prepared using the 2022 Methodology.

The Mutual Evaluation Report identifies the strengths and weaknesses of Belgium's AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance, and recommended actions for improvement. The highest priority measures are identified as Key Recommended Actions (KRA) and included in this KRA Roadmap.

Based on Effectiveness and Technical Compliance Ratings, Belgium is placed in enhanced follow-up. This KRA Roadmap also serves as the basis for Belgium's follow-up process.

Belgium should:

Immediate Outcome 1 (Risks, policy and coordination)

a) Increase the expertise of all competent authorities in the use of virtual assets for ML/TF purposes, based on existing experience, in order to improve the understanding of the risks associated with this sector, assess them at their relevant level for ML and for TF at national level, and define an appropriate strategic, legislative/regulatory and operational framework to improve the management of these risks.

b) Refine the mapping of alternative financial channels (e.g. cash, informal remittance systems) existing in the country and estimate their weightings so as to better highlight the ML/TF risks posed by these channels and take the necessary measures to manage them at national level.

c) Adopt an AML strategy based on the strategic priorities for Belgium, targeting major crime patterns (such as professional money launderers and the use of virtual assets), and link it with the existing strategies designed to counter predicate offences in the country, in order to stem the growing links between ML and organised crime.

Immediate Outcome 2 (International cooperation)

d) Accelerate activities designed to facilitate international cooperation with countries outside the EU by involving, together with the SPF Justice, as necessary, the judicial and diplomatic authorities, in order to enhance the interactions with countries with which Belgium shares the most links, and in areas of major crime for Belgium.

e) Collect the necessary statistical data on mutual legal assistance and other forms of formal cooperation, in order to better measure its effectiveness, promote activation of international cooperation, promote the results obtained in major cases and identify the best practices.

f) Increase the judicial authorities' resources to enable them to pursue systematically the international ramifications identified in ML cases, including through support from SPF Justice.

Immediate Outcome 3 (Financial sector and virtual asset supervision and preventive measures)

g) Adopt, as soon as possible, a legislative or regulatory framework designating the competent authority for the licensing and supervision of VASPs, in accordance with the requirements of the MiCA regulation (in relation to the technical compliance deficiencies identified in R. 15 - see the TC Annex).

h) Implement the administrative sanction powers of the BNB and the FSMA, in particular by adapting human resources and, where necessary, the legislative framework, to ensure that their action has a truly dissuasive effect. These sanctions should be published, accessible and by name.

Immediate Outcome 4 (Non-financial sector supervision and preventive measures)

i) Introduce more frequent inspections in the highest-risk sectors (diamond dealers, estate agents and business centres) by increasing the number of on-site inspections and ensuring regular monitoring; as well as by systematically standardising preparations for inspections in order to allocate the appropriate resources to each supervisory activity based on risks.

j) Strengthen the sanctions regime in all DNFBP sectors to ensure a proportionate and dissuasive response, particularly to serious breaches, including by applying the full range of sanctions available, and by publishing decisions by name to reinforce their dissuasive effect.

k) Strengthen the capacity of SPF Economy in the area of AML/CFT and ensure that AML/CFT issues are fully integrated into all its activities, in order to optimise awareness among the entities under its responsibility.

Immediate Outcome 5 (Transparency and beneficial ownership)

l) Apply risk-based mechanisms for verifying the information to be recorded in the Banque-Carrefour des Entreprises and Ultimate Beneficial Owners (UBO) registers, to ensure their reliability and mitigate the risks of the creation of legal persons for ML/TF purposes (in relation to the technical compliance deficiencies identified in R. 24 - see TC Annex).

m) Accelerate the implementation of ongoing measures to update the registers (e.g. judicial dissolution of shelf entities, processing of the stock of notifications of discrepancies, and targeted checks of data in the UBO register) in order to improve the reliability of the data currently recorded in the registers.

n) Adopt the necessary measures to ensure greater transparency in the use of nominee directors and shareholders to prevent and tackle the abuse of these mechanisms and facilitate the detection of straw men, while developing a large-scale awareness of the risks associated with straw men.

Immediate Outcome 7 (Money laundering investigations and prosecutions)

o) Allocate resources and effective technological tools to the authorities responsible for the investigation and prosecution of ML, commensurate with the threats identified, in order to tackle the polycriminal networks involved in ML.

p) Implement a proactive strategy for identifying ML and define a criminal justice policy that directs investigations and prosecutions towards complex ML cases with significant profits, in line with the ML risks identified, by relying on established jurisprudence on ML evidence (reversal of the burden of proof of the illegal origin of funds) and by enhancing providing the Federal Prosecutor's Office attributions with additional powers in to prosecute the most complex ML cases to optimise handling of these cases.

q) Ensure that deterrent sanctions are imposed on criminals convicted for ML offences and restrict the use of the transaction procedure in ML cases, which must not replace criminal prosecution and must include guarantees of transparency and public disclosure of the agreements reached.

Immediate Outcome 8 (Confiscation)

r) Apply a criminal justice policy that prioritises financial investigations in ML cases with high recovery potential, even where assets are not immediately available and accessible assets are identified at the start of the investigation, in line with the ML risks identified in the country.

s) Allocate the necessary human and technological resources to law enforcement authorities, prosecutors investigation and prosecution authorities and the Central Office for Seizures and Confiscations (Office central des saisies et confiscations), so that they can conduct more systematic and thorough financial investigations and criminal investigations to enforce confiscation measures ("enquête pénale d'éxecution") and effectively confiscate criminal assets, including in complex ML/TF cases with a transnational dimension and/or involving virtual assets.

t) Implement a strategic approach, backed by the necessary resources, to target customs controls of accompanied and unaccompanied movements of cash and BNIs more effectively and to use information from customs and police authorities on cross-border cash transportation more strategically, with a view to obtaining bringing confiscations results to a level commensurate with the identified risks of cash trafficking to which Belgium is exposed.

Immediate Outcome 10 (Terrorist financing preventive measures and financial sanctions)

u) Remove the requirement of the existence of a police or judicial information or investigation from the designation criteria, so that persons and entities can be targeted more actively (in line with the technical compliance shortcomings identified in R.6 – see TC Annex).

v) Strengthen inter-institutional coordination between competent authorities, for example by considering the designation of a point of contact responsible for coordinating and monitoring the NPO sector within the CFT framework, in order to ensure a coherent overview, facilitate the sharing relevant information and allow for a more structured, targeted and proportionate manner monitoring of the TF risks identified.

w) Define and implement proportionate and targeted monitoring and mitigation measures for NPOs identified as being at high TF risk, taking account of the structural and operational features of the non-profit sector (in line with the technical compliance shortcomings identified in R.8 – see TC Annex).

Immediate Outcome 11 (Proliferation financing financial sanctions)

x) Deepen the national proliferation financing (PF) risk analysis on the basis of a contextual analysis of the different methods, trends and complex typologies related to non-compliance with, non-application of or the evasion of targeted financial sanctions (TFS) for PF, and involve the private sector.

y) Develop and apply risk indicators to enable financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), and customs and supervisory authorities to identify complex patterns of evasion of targeted financial sanctions for PF.

z) Conduct inspections of FIs and DNFBPs in relation to PF TFS, targeting not only the mechanisms in place but also the effective detection of any failures to comply with freezing obligations, and provide for appropriate sanctions for any failures identified.

Preface

This report summarises the anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CFT/CPF) measures in place as of the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT/CPF system and provides recommendations on how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the 2022 Methodology. It was based on information provided by the country's authorities and information obtained by the evaluation team during its on-site visit in Belgium (27 January to 14 February 2025).

The evaluation was conducted by an assessment team consisting of[2]:

- Chantal Goupil, FINTRAC, Canada
- Marie-Laure Paldi, ACPR, France
- Gérard Sautebin, Prosecutor's Office of the Swiss Confederation
- Michel Turk, Bureau de gestion des avoirs, Luxembourg
- Lucía Villavieja Urzainqui, SEPBLAC, Spain

with the support of the FATF Secretariat represented by Anne-Françoise Lefèvre, Masha Rechova and Lise Smith, accompanied by Karnon Lofigue from the GIABA Secretariat.

The report was reviewed by Jean-Pierre Brun (World Bank), Nuno Matos (Portugal) and Irina Talianu (MONEYVAL Secretariat).

Belgium previously underwent a mutual evaluation during the fourth round of FATF mutual evaluations in April 2015, conducted according to the 2013 FATF Methodology. The 2015 evaluation and the 2018 Follow-Up Report with technical compliance re-ratings have been published and are available at https://www.fatf-gafi.org/fr/countries/detail/Belgique.html.

This mutual evaluation concluded that Belgium was compliant (C) with 11 Recommendations, largely compliant (LC) with 18 Recommendations, and partially compliant (PC) with 11 Recommendations. Belgium's effectiveness was rated as Substantial for four Immediate Outcomes and Moderate for seven Immediate Outcomes.

Based on these results,[3] Belgium was placed under enhanced follow-up measures. Since the 2015 evaluation, Belgium has been reassessed for its technical compliance vis-à-vis 15 Recommendations:

- 5 Recommendations re-evaluated from PC to LC: R.8, R.17, R. 18, R.28 and R.33;
- 3 Recommendations re-evaluated from PC to C: R.12, R.16 and R.26;
- 7 Recommendations re-evaluated from LC to C: R.1, R.2, R.10, R.15, R.19, R.27 and R.35.

A total of three Recommendations (R. 6, R.7 and R.13) remain rated at PC level since the 2015 evaluation. Belgium remained under enhanced follow-up for its effectiveness shortcomings.

[2] Camille Cruel of the Hamburg State Criminal Police (Germany) took part in the pre-on-site phase of the mutual evaluation.

[3] See FATF Fourth Round Procedures, para 89.

Introduction to money laundering and terrorist financing risks and context

51. The Kingdom of Belgium is located in the heart of Western Europe. It lies on the North Sea and shares borders with The Netherlands, Germany, Luxembourg and France. It covers an area of 31 000 km2 and has a population of more than 11 million[4]. In 2023, the gross domestic product (GDP) was EUR 614 billion. Brussels is the capital of Belgium.

52. Belgium is a constitutional monarchy and a Federal State consisting of communities and regions. The King is the Head of State but does not hold executive power. Federal executive power is held by the Prime Minister and his or her government. The legislative powers are divided between the Federal Parliament, which is made up of the Senate and the Chamber of Representatives, and the Federal Government, made up of the King and the appointed ministers.

53. The Federal Government's authority covers areas such as foreign affairs, national defence and justice, and includes anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CFT/CPF) measures. The Belgian population is divided into three language groups: Dutch-speaking, French-speaking and German-speaking. These groups are institutionally organised into three communities: Flemish, French and German-speaking. Belgium also has three economic regions: Brussels-Capital, Flanders and Wallonia. Each region and community have the executive and legislative power to pass measures (decrees, orders) that are legally binding in areas within the scope of their authority. Because the regions have the authority to grant export licenses for weapons or goods that can be used for civil or military purposes, they play a role in countering proliferation financing (PF) of weapons of mass destruction.

54. Belgium is one of the six founding Member States of the European Union (EU) and a member of the Eurozone since 1999. The European Commission and most Community institutions are headquartered in Brussels. The AML/CFT regime in Belgium is based on a legal framework defined both at the national and European level.

[4] Statistical themes - Eurostat (europa.eu)

ML/TF/PF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF/PF Risks

55. According to the Belgian Federal Police, the main criminal activities in Belgium are, in order of importance: illicit drug trafficking (24.09%), theft and acts of violence, computer fraud, human trafficking and smuggling, and terrorism.[5]

56. Belgium's strategic geographical location makes it a major commercial crossroads. The port of Antwerp-Bruges is the second-largest port in the EU, covering more than 800 destinations worldwide, and handling around 290 million tonnes of sea freight per year, corresponding to 4.5% of Belgian GDP.[6] As a result, it is also of interest to criminals, as the large volumes of imports and exports mean that illicit goods are less likely to be discovered there. In 2024, Belgian Customs made a total of 134 cocaine seizures, amounting to more than 44 tonnes (after a record-breaking 121 tonnes in 2023,[7] and more than 280 tonnes in the last three years).[8] In this context, and as the Belgian authorities acknowledge, dockers and civil servants are specifically targeted or likely to be targeted by offers of corruption.

57. According to Europol, more than one hundred cross-border criminal networks are active in Belgium.[9] Organised crime takes many forms and is particularly prevalent in areas such as drug trafficking, smuggling and money laundering. Human trafficking and "grey marriages"[10] are other activities carried out by the networks mapped in Belgium. Criminal networks practising extortion and blackmail on small businesses and local shops (especially those operating with cash, such as restaurants or night shops) are also active in Belgium. Trafficking in drugs, especially cocaine, remains one of the main activities of criminal networks in Belgium (see figures above relating to the port of Antwerp). Belgium is also one of the main centres of amphetamine production in Europe.[11]

58. Criminals use legitimate businesses as cover for their criminal operations. The construction, property, hotel and logistics sectors are the main targets. The main characteristic of these criminal networks operating in Belgium is their multi-nationality. They are composed mainly of Belgian and Dutch nationals, but also include Albanians or associates from other countries in the Western Balkans, Turkey or Morocco.[12]

Belgium's risk assessment and scoping of higher-risk issues

59. As part of the EU, Belgium is covered by the supranational risk assessments carried out by the European Commission in 2017, 2019, and 2022 and contributed to their development.[13]

---

[5] Source: GES-ITINERA, 8 April 2024, breakdown of police investigations opened in 2023, by phenomenon

[6] World port | Port of Antwerp-Bruges

[7] Less cocaine seized in the port of Antwerp, more seizures in Latin America | News.belgium :https://news.belgium.be/fr/moins-de-cocaine-saisie-dans-le-port-danvers-plus-de-saisies-en-amerique-latine Cocaine trafficking via the port of Antwerp: annual figures from the Federal Police and the Justice Department | Police Fédérale https://www.police.be/5998/fr/actualites/trafic-de-cocaine-via-le-port-danvers-chiffres-annuels-de-la-police-federale-et-de-la

[8] Press conference on drugs:Results 2024 in the Port of Antwerp - Customs and Excise, SPF Finance, January 2025

[9] Decoding the EU's most threatening criminal networks

[10] Fraudulent marriages in which only one party is aware of the fraud

[11] Drug supply, production and precursors – the current situation in Europe (European Drug Report 2024) https://www.euda.europa.eu/publications/european-drug-report/2024/drug-supply-production-and-precursors_fr

[12] Information from the Belgian authorities, contribution for Introduction.

[13] The next risk assessment under the old EU framework is to be prepared in 2025. Belgium will also be involved in the Union risk assessment to be developed according to the new requirements of Directive (EU) 2024/1640 (the "6th AML/CFT Directive").

Main conclusions of national risk assessments

60. The 2023 Money Laundering National Risk Assessment (ML NRA)[14] states that Belgium is mainly exposed to criminal threats associated with cash trafficking, drug trafficking, social and tax fraud, other types of fraud and organised crime. Belgium's ML environment is marked by a high degree of interconnection between criminal activities, which increases the opacity of the schemes and modus operandi leading to ML activities. Criminals tend to invest in sectors and activities not covered by the scope of the AML regime, (e.g. the use of cash, cross-border cash transportation or alternative money transfer channels), which increases the complexity of ML circuits and makes them less visible to the authorities.

61. The ML NRA's conclusions identify the main ML risks in the country as being:

- the preponderance of cash, both in sectors of activity such as construction, industrial cleaning, night-time grocery shops, traders in precious materials, and in informal sectors such as unofficial cash couriers (hawala), or cross-border cash transportation;
- the role of money laundering professionals (individuals, organisations or networks involved in money laundering activities on behalf of third parties for a fee or on commission) who use the offsetting technique to set up fully fledged networks (notably the "Brazilian" and "Romanian" networks), in which the money laundering stems from various criminal activities (cash generators) including drug trafficking, fraud, illicit trafficking in goods and merchandise and "Trade Based Money Laundering" (TBML) operations, generally with Asian countries;
- assistance and services for companies, including the creation of corporate structures and assistance in tax and accounting matters from professional accountants;
- fictitious legal structures, shell companies and dormant companies, generally established in connection with social and tax fraud and organised crime;
- real-estate investments in Belgium or abroad;
- investments in safe-haven assets such as diamonds, precious metals and high-denomination bank notes;
- the use of virtual IBANs, and specifically the issuance of virtual payment account numbers solely for the purpose of redirecting payments to a physical payment account linked to an ordinary IBAN. A virtual IBAN marked "BE" can be used by people or entities who are not customers of a Belgian or even an EU financial institution. The presence, albeit of a limited number, of Belgian institutions that actively issue virtual IBANs in ways that expose them to high ML/TF risks increases the risk for the Belgian market.

62. Belgium considers sectors that make extensive use of cash, notably hotels/restaurants/coffee places ("HORECA"), construction, industrial cleaning, money transfer and virtual currency sectors as being subject to a major or substantial level of ML risk. It also pays particular attention to diamond traders, safe deposit box rental operators outside the financial sector, football clubs, and the financial and insurance sectors.

63. The 2023 Terrorist Financing National Risk Assessment (TF NRA) concluded that the main threat is from ex-foreign terrorist fighters or radicalised individuals through micro-financing involving new payment methods and small cash transactions, mainly of legal origin.[15] It also highlights the growing links between organised crime and TF, mainly through drug trafficking.

64. The 2024 Proliferation Financing National Risk Assessment (PF NRA) concluded that Belgium is relatively unexposed to the risk of direct proliferation financing programmes, insofar as all financial flows involving natural and legal persons from countries under international sanctions are tightly controlled.

[14] Summary (in French) NRA_2023_Synthèse_ML.pdf

[15] Summary (in French) NRA_2023_Synthèse_FT.pdf

According to the NRA, in most cases, the various threats (non-compliance/circumvention of targeted financial sanctions, use of shell companies, state actors, cyber attacks, and North Korean ships, population, workers and diplomatic personnel) and vulnerabilities (institutional and legislative frameworks, maritime sector, sectors at risk of ML/TF, attempts to acquire expertise and technologies, liquidity) are counterbalanced by mitigating measures that reduce the residual risks without completely eliminating them.[16]

Areas of higher risk identified in the scoping note

65. In the scoping note, the evaluation team identified areas subject to a higher ML/TF risk or of particular importance in the Belgian context:

- *Identifying and understanding risks* – The evaluation team took a closer look at the risk identification and detection process, particularly for ML risks, by examining the sources used by the Belgian authorities to ensure that they are capable of measuring and identifying the main ML phenomena that develop outside the regulated AML/CFT field and the reporting entities. It also examined the impact of these parallel circuits on the detection of ML.
- *Banking sector and financial activities with a high ML/TF risk* – Given the importance of the banking sector in the national financial system, and although the ML NRA retains a residual Moderate level of ML risk, the evaluation team paid specific attention to the sector's activities, especially correspondent banking and wealth management, which are more highly exposed to ML risks. In addition, the team paid particular attention to the measures targeting currency exchange offices and remittance service providers, due to the high TF risk.
- *Use of cash and related elements (offsetting techniques, money laundering "professionals") for ML purposes* – The evaluation team paid particular attention to mechanisms favouring the offsetting technique facilitated by the circulation of cash, and the means applied to prevent and eradicate it: limiting the use of cash, links with the fight against abuse of corporate vehicles and against social and tax fraud, prevention of the misuse of professionals subject to AML/CFT obligations by "professional money launderers", controls on company service providers.
- *Use of innovative financial operators and services for AML/CFT purposes* – The evaluation team examined the mechanisms that enable criminals to misuse innovative media such as virtual currencies, e-IBANs and products based on new financial technologies (fintech) for ML/TF purposes, including by examining the measures adopted to identify, supervise and control these activities for AML/CFT purposes, and to ensure that the arrangements in place remain relevant to the developments in the sector.
- *Abuse of legal persons for ML* – The evaluation team studied the typologies and patterns of abuse of legal persons and examined the prioritisation of this field by the Belgian authorities. It also examined the close links with other criminal activities, such as social or tax fraud or the activities of "professionals" who facilitate ML operations. It also reviewed the measures taken to increase the transparency of legal persons and, where necessary, to identify them rapidly and wind them up. It also considered how the simplification measures introduced by the 2019 Belgian Companies and Associations Code maintain stringent transparency requirements to prevent abuse.
- *Designated non-financial businesses and professions at high risk of ML/TF* – The evaluation team focused on non-financial sectors that are subject to the AML/CFT regime but remain at high risk of misuse for ML/TF purposes: diamond dealers and professionals in the real estate sector. It focused on the understanding of ML/TF risks – both by reporting entities and supervisory authorities – and the specific measures taken to manage these risks, as well as their implementation and oversight by competent authorities, including the initiatives envisaged to strengthen this supervision.

[16] Summary Conclusions_FP_FR.pdf

- *Investigation and prosecution of ML* – The evaluation team examined how the Belgian investigation and prosecution authorities detect, prioritise and tackle the ML component associated with the main criminal activities leading to ML, particularly in the complex schemes identified, involving activities linked to organised crime and commercial operations (TBML), especially cross-border activities (e.g. the Sky ECC case). It also set out to understand the terms and conditions attached to transaction procedure, which prosecuting authorities have been using to resolve ML cases since 2017.
- *TF schemes and vehicles* – The evaluation team examined the resources used by Belgium to tackle the new approaches to TF based on micro-financing, and how the authorities identify, detect and prosecute these criminal activities, particularly in terms of coordination and exchanges of intelligence, both nationally and internationally. In this respect, the evaluation team also examined Belgium's response on TF aspects to the terrorist attacks of 2016 and 2023, and to those of 2015 in France, which had numerous links with Belgium.

66. The evaluation team paid less attention to activities with lower ML/TF risks, due to their smaller volumes of activity, lesser importance in the Belgian economic and financial landscape and the characteristics of their activities that significantly reduce their exposure to abuses for ML/TF purposes: bailiffs, mutual guarantee companies and independent financial planners.

Materiality

67. Belgium is an open and highly service-oriented economy, with the service sector accounting for 85,6% of value added in 2023.[17] The Belgian economy has an openness rate[18] of 88%, which reflects the importance of trade to the country.[19] In 2023, 63,8% of Belgian exports were destined for the intra-European market, with the main trading partners being Germany, France and the Netherlands.[20]

68. The use of cash by consumers continues to decline in Belgium. Cash payments accounted for 57% of transactions at physical points of sale in 2019, 45% in 2022 and an estimated 39% in 2024.[21] This trend reflects consumers' growing preference for digital payments. In addition, all retailers have been required to offer their customers a digital payment solution since 2022.[22]

69. Regarding the underground economy, which in Belgium essentially concerns moonlighting, i.e. work that is undeclared for social security and tax purposes, one study estimates that it amounted to around 3.48% of total GDP in 2012.[23]

Financial sector and VASPs

Main characteristics, weighting and materiality of the various financial sectors and VASPs

70. The Belgian financial sector is largely based on four major banking groups, which are active internationally, particularly in Central and Eastern Europe, but also in the Netherlands and Germany. In the

[17] Overview of economic activity in Belgium | SPF Economy

[18] Measurement of a country's participation in international trade in goods and services

[19] Economic indicators for Belgium | SPF Economy

[20] Belgian Trade - Belgian Foreign Trade Agency

[21] Study on the payment attitudes of consumers in the euro area (SPACE)

[22] art. VI.7/4, Belgian Code of Economic Law, Obligation to offer an electronic means of payment | SPF Economy

[23] https://socialsecurity.belgium.be/fr/activites-internationales/ampleur-de-la-fraude-sociale-et-fiscale-sublec#:~:text=Pourtant%20on%20peut%20estimer%20que,4%25%20du%20PIB%20en%20France

Belgian economy, the combined assets of these four Belgian banks amounted to almost EUR 1,000 billion in assets in 2024 – around 171% of Belgian GDP and 87% of the total banking sector (EUR 1,211 billion).[24]

71. The Belgian financial sector is also highly integrated into the European single market, benefiting from the mutual recognition principle, which allows financial institutions from other EU or European Economic Area (EEA) Member States to set up business or operate in Belgium without requiring additional authorisation from the Belgian authorities ("European passport").[25] The Belgian banking sector is highly internationalised, much more so than in neighbouring countries.[26] Of the 80 or so banks operating in Belgium in 2024, 62 – around 80% of them – are subsidiaries or branches of foreign groups, compared with 59% in the Netherlands, 39% in France and 10% in Germany.[27]

72. Brexit has had a significant impact on the Belgian financial sector, as it led to the loss of the "European passport" for UK financial institutions and required them to establish a presence in an EU Member State to enable them to keep serving their European customers. This situation has led some of these institutions to relocate some or all of their activities to EU countries, including Belgium. This movement has led the National Bank of Belgium (BNB) to supervise new financial players, mainly in the payment institutions and electronic money sectors.

73. The Belgian insurance market has grown significantly in recent years. In 2024, the sector recorded total premium income of EUR 35.1 billion, up 8.4% on 2023, an increase mainly attributed to growth in individual life insurance policies.[28] 4,835 insurance intermediaries were registered in Belgium (and subject to AML/CFT obligations) by 31 December 2024, with life insurance assets under management reaching EUR 16.4 billion in 2023 (or 2.68% of GDP).

74. The collective investment undertakings (OPC) sector in Belgium is enjoying sustained growth, reflecting investors' continuing interest in these collective investment vehicles.[29] It has 267 active entities, including 36 from the EEA. Over 2023 as a whole, the Belgian fund market recorded growth of 12.4%, for an increase of EUR 30 billion[30] with a total of EUR 229.06 billion under management, corresponding to almost 40% of Belgian GDP.

75. The payment institution (PI) sector is undergoing strong growth, with 52 active entities in 2024. PIs offer digital services (accounts, terminals, online payments), often without a physical presence. In 2024, they handled EUR 256.61 billion in transactions.

76. Eight *currency exchange offices (bureaux de change)* were operating in Belgium in 2024. Trading volumes reached EUR 190 million (0.031% of GDP).

77. Five electronic money institutions (EMIs) were operating in Belgium in 2024, including one under the "European passport" scheme. Their services, including digital wallets and online payments, are fully digitised. The volume of transactions reached EUR 4.26 billion, for a total balance sheet of EUR 2.85 billion.

78. The lenders sector includes several categories of players who carry out their activities within credit institutions (for the most part), or in subsidiaries, but also in smaller entities. They offer different types of lending services – mainly mortgages and consumer loans. 166 licences to carry out lending activities were active in 2024 (the same legal entity may hold both a consumer credit and a mortgage credit licence) and represented an estimated volume of credit granted in 2023 of EUR 451.66 billion, corresponding to 73.56%

---

[24] Quarterly and annual aggregates:GDP expenditure

[25] What is a "European passport"? | FSMA

[26] https://febelfin.be/media/pages/cijfers/2023/2acc078274-1725627304/facts-figures-fr-2023.pdf?

[27] Number of registered credit institutions

[28] https://press.assuralia.be/marche-belge-de-lassurance--un-appetit-accru-pour-les-assurances-vie-individuelles-en-2024?

[29] These organisations enable investors to pool their capital and invest it in a variety of assets, such as equities, bonds or property.

[30] https://febelfin.be/en/press-room/saving-investing/figures-ucits-sector-4th-quarter-of-2023?

of GDP. Depending on their status and activities, lenders are subject to AML/CFT supervision by the National Bank of Belgium (BNB) or the Financial Services and Markets Authority (FSMA) (see table below). The stock held by non-bank lenders, some of which are under the AML/CFT supervision of the BNB and some of which are under the AML/CFT supervision of the FSMA, amount to EUR 83.02 billion (13.52% of GDP), EUR 57.02 billion (9.28% of GDP) of which are held by lenders under the AML/CFT supervision of the FSMA.

Table 0.1. Financial Institutions

Obliged entity/sector	Number of entities[31]	Balance sheet/outstanding/products issued 2024 (EUR)	AML/CFT supervisory authority[32]
Credit institutions (CI) (Art. 5, §1, 4°)	76 (including 45 EEA, 4 TC)	Balance sheet: 1,211 billion *(197% of GDP)* Transactions (2023): 17,500 billion	National Bank of Belgium (BNB)
Payment institutions (PI) (Art. 5, §1, 6°)	52 (including 18 EEA)	Balance sheet: 15.78 billion Transactions: 256.61 billion	
Electronic money institutions (EMI) (Art. 5, §1, 7°)	5 (including 1 EEA)	Balance sheet: 2.85 billion Transactions: 4.26 billion	
Life insurance companies (Art. 5, §1, 5°)	34 (including 10 EEA)	Balance sheet: 311 billion Net premiums underwritten: 17 billion	
Central security depositories (Art. 5, §1, 8°/1)	2	Balance sheet: 161.6 billion	
Mutual guarantee companies (Art. 5, §1, 9°)	4	Balance sheet: 12.2 million	
Stockbroking firms (Art. 5, §1, 10°)	19 (including 9 EEA)	Balance sheet: 0.7 billion Under management: 5.8 billion	
Investment management and investment advisory companies (Art. 5, §1, 11°)	35 (including 19 EEA)	Under management/ advisory services: 10.74 billion (*1.75 % of GDP*)	Financial Services and Markets Authority (FSMA)
Collective investment undertakings[33] (Art. 5, §1, 12° et 13°)	284 (including 27 EEA)	Under management: 231.82 billion (37.75% of GDP)	
Currency exchange offices (Art. 5, §1, 16°)	8	Transactions: 0.19 billion (0.031% of GDP)	
Market operators (Art. 5, §1, 15°)	1	Average daily transactions: 0.32 billion *(13.37% of GDP on an annual basis*)	
Banking and investment service brokers (Art. 5, §1, 17°)	17	Total amount covered by regulated services: 0.5 billion *(0.080% of GDP*)	
Independent financial planners (Art. 5, §1, 18°)	4	Total amount covered by regulated services: 0.18 billion *(0.028% of GDP*)	
Insurance intermediaries (Art. 5, §1, 19°)	4,835 (including 1 EEA)	Assets under management (2022): 16.4 billion *(2.68% of GDP*)	
Lenders (excluding lenders supervised by the BNB) (Art. 5, §1, 20° juncto Art. 85, § 1, 4°)	101	Outstanding loans: 57.027 billion (9.28% of GDP)	

[31] The number in brackets indicates how many of these entities are branches or agents governed by the law of another country in the European Economic Area (EEA) or a country outside the EEA (third country)

[32] List of supervisory authorities: see Art. 85 of the Belgian AML Law

[33] This category includes collective investment undertaking (CIU) management companies, which administer these funds in accordance with defined investment strategies; alternative collective investment undertakings, which offer investment strategies that differ from traditional CIUs; and institutional debt investment companies, which specialise in acquiring debt held by institutions. Of the latter, those that grant mortgages are classified as lenders.

Obliged entity/sector	Number of entities 31	Balance sheet/outstanding/products issued 2024 (EUR)	AML/CFT supervisory authority 32
Bpost[34] (Art. 5, §1, 3°)	1	Transactions: 0.8 billion *(0.14% of GDP)*[35]	Treasury (SPF Finance)
Finance leasing and leasing companies (Art. 5, §1, 21°)	116	Loans granted in 2022 : 5 billion	SPF Economy

Source: Belgian authorities

79. At the time of the on-site visit, no virtual asset service providers (VASP) were registered or licensed in Belgium.

80. Following the transposition of European legislation,[36] the AML/CFT provisions were extended in 2022 to include activities involving exchanges between virtual money and fiat money, in addition to custodian portfolio services (Royal Decree of 8 February 2022). Belgium then introduced a transitional regime for entities that were already carrying out these activities. Subject to certain conditions, entities could temporarily pursue their activities pending a decision by FSMA on their application for registration. The FSMA received 14 applications for registration and found that nine VASPs met the conditions required to benefit from the provisional regime. At the end of the transitional period, the FSMA did not register any of the VASPs due to shortcomings in the registration files and/or voluntary withdrawals of registration applications by VASP candidates (see IO.3).

Table 0.2. Virtual asset service providers

Obliged entity/sector	Number of entities	Balance sheet/outstanding/products issued 2024 (EUR)	AML/CFT supervisory authority
Providers of services for exchanges of virtual and legal currencies (Art. 5, §1, 14°/1)	0	NA	Financial Services and Markets Authority (FSMA) (until the end of December 2024)
Custodian portfolio service providers (Art. 5, §1, 14°/2)	0	NA	

Source: Belgian authorities

Materiality

81. The evaluation team applied the following weightings to assess the implementation of preventive measures by FIs and VASPs: *very great importance* for credit institutions, payment institutions and VASPs; *great importance* for currency exchange offices and life insurance companies; *moderate importance* for lenders, insurance intermediaries, electronic money institutions, collective investment undertakings and Bpost; and *low importance* for other FIs.

Very great importance

82. **Credit institutions** (CIs) – Credit institutions in Belgium offer a very wide range of products and services, exposing the sector to varying degrees of ML/TF risk depending on their activities. Fifteen or so

[34] Bpost's liability under the Belgian AML Law is limited to its activities in the field of postal financial services and the issue of electronic money

[35] Turnover from activities subject to AML/CFT regulations (postal financial products: State postal current accounts, postal payments, postal assignments, "bpaid" prepaid credit card): EUR 47 million

[36] Transposition of Article 1(1)(c) of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and Directives 2009/138/EC and 2013/36/EU ("AMLD 5 Directive").

banks also offer correspondent banking services (four of them for very significant amounts) and pose a particularly high risk. The Belgian banking landscape is dominated by a small number of players, with the four largest banks accounting for 87% of assets (see above). Twenty-two institutions are also active in international trade (four of which account for 87% of transactions) and 13 institutions specialise in asset management (EUR 91.6 billion in assets, with four players responsible for nearly 90% of this volume). Given the size of the sector, the concentration of risky activities and the exposure to international financial circuits, this sector is considered to be of substantial importance in terms of AML/CFT.

83. **Payment institutions** (PIs) **-** The PI sector is increasingly exposed to ML/TF risks, especially due to the digitalisation of services, which can be accessed remotely, and their speed and ease of access. Some PIs offer high-risk services, such as fund transmissions – as distinct from simple transfers – often carried out without opening an account, with large cash flows and a predominantly occasional customer base. The use of networks of agents, who are themselves not reporting entities, increases the sector's vulnerability, especially for activities which are "passported" from other Member States. Their vulnerabilities have been exacerbated by the development of new services such as virtual e-IBANs and the presence of major players following Brexit, which "passport" their activities throughout the EU from Belgium. This has required intensive monitoring and the implementation of measures by the supervisory authority due to initially limited local governance structures. PIs are the second-largest category of FI in terms of the number of suspicious transaction reports (STRs) sent to the FIU (CTIF), most of which are issued by a single PI. The PIs with the largest market shares – and therefore the highest exposure to ML/TF risks – have been subject to at least one on-site inspection, while those categorised as standard to low risk are subject to off-site supervisory measures according to a risk-based approach, and are not sufficiently inspected (see IO.3). Despite remaining quite small compared to CIs, the materiality of this sector is high, due to its structural vulnerabilities and the profile of its services.

84. **Virtual asset service providers** (VASPs) – In 2022, around 4% of the Belgian population declared that they own virtual assets, reflecting the rapid growth of this ecosystem. The risks associated with the circulation and use of virtual assets are considered major in Belgium, both for ML and TF. These risks are identified in national risk assessments, and their significance is spontaneously mentioned by Belgian authorities and the private sector. Belgium also reports confirmed cases of the use of virtual assets for ML and TF purposes (see IO.7). The growing use of virtual assets in ML and TF cases therefore poses a major challenge, especially as the investigation and prosecution services still suffer from limited resources and insufficient access to the specialised technical tools needed to track and analyse these flows. There are currently no registered players (see IO.3), but the FSMA, the competent authority for licensing and supervising VASPs until December 30, 2024, has received 14 requests for provisional authorization, of which 9 have been granted. Given this sector's rapid expansion and high inherent risk exposure, virtual asset activities must therefore be considered of the utmost importance in AML/CFT assessment, especially as there is currently no effective regulatory framework to ensure appropriate supervision.

Great importance

85. **Currency exchange offices**– Although they are few in number (8) and account for a relatively low volume of transactions, the authorities identify currency exchange offices as posing a high residual ML/TF risk, particularly due to their high exposure to threats and vulnerabilities such as the intensive use of cash, the difficulty of determining the origin of funds due to the occasional nature of transactions, and the risk of dividing up transactions to avoid identification. Some players combine this activity with gold trading,[37] which increases their exposure. There is still room to improve the preventive measures implemented, and reporting activity varies greatly from one year to the next (see IO.3), which raises questions about the robustness of their due diligence system. Despite strict supervision by the FSMA and regular checks and

[37] Gold trading is not subject to the FSMA's AML/CFT supervision. However, FSMA takes it into account when assessing risk.

inspections, the impact of supervision on the sector's AML/CFT compliance remains insufficient. Because of its inherently high risk profile, this sector is considered to be highly material in the AML/CFT field, despite its small size.

86. **Life insurance companies -** Despite remaining limited in number (34 institutions), these companies manage very substantial financial volumes (see above). The sector is seeing an increase in recourse to products that are riskier than guaranteed-rate products, such as policies linked to investment or capital bond funds. The underwriting of the riskiest products (i.e. individual life insurance, investment fund-type products (class 23) and capital bond products (class 26)) accounted for EUR 3.8 billion and EUR 770 million respectively in premium income at the end of 2024 (estimated value). The use of certain life insurance products for self-laundering purposes was highlighted by CTIF in 2023, and the BNB's 2023 Sectoral Risk Analysis (SRA) takes this into account.

Moderate importance

87. **Lenders** – This sector is highly concentrated within credit institutions and subsidiaries of credit institutions. Risks within the sector vary: mortgage lenders pose a more limited risk, while consumer credit lenders are riskier from a TF point of view, due to the nature of the products (lenders offering prepaid credit cards fall under the AML/CFT supervision of the BNB), although the TF mechanism associated with cash couriers linked to loans has become less important according to the TF NRA, and the TF mechanism linked to the non-repayment of loans has not been detected in recent years. This sector is supervised by the FSMA, which applies risk-based controls.

88. **Insurance intermediaries –** Insurance intermediaries are supervised by the FSMA and are subject to a specific AML/CFT supervisory approach due to their large number, their lower risk profile and the presence of many small players. The inspections show an improvement in risk management, despite certain persistent weaknesses in the understanding of certain specific risks and in the implementation of preventive measures. Several applications for registration have been refused in this sector on grounds of the "fit and proper" criterion, but this number remains marginal given the size of the sector. The importance of insurance intermediaries in ML/TF remains limited, notably because financial flows transit almost exclusively to and from the insurer and are easily traceable, which explains why these players are seldom, or never, included in the money laundering typologies. This sector is therefore classified as being of moderate materiality.

89. **Electronic money institutions** (EMIs) – These institutions remain relatively small compared with PIs, but have a significant volume of business (see above). The sector includes one significant player as a result of Brexit, which "passports" its activities within the EU from Belgium via networks of agents, which may in some cases complicate national supervision. Electronic money cards are highly portable and offer a certain degree of anonymity, although this is capped at EUR 150. These features raise doubts about traceability, particularly in the event of top-ups in cash or by other anonymous cards. The number of STRs has increased tenfold in recent years, as a result of an inspection carried out in 2019 by the BNB at the main EMI operating from Belgium. The risk profile of EMIs therefore needs to be monitored. Although the sector remains limited in size, the presence of cross-border players justifies its classification as a sector of moderate materiality vis-à-vis AML/CFT issues.

90. **Alternative collective investment undertaking (OPCA management companies, OPCs and institutional debt investment companies ("*sociétés d'investissement en créances* – SICs")**– This sector accounts for significant financial volumes (see above). It brings together a wide range of players with varied risk profiles and a wealthy clientele. Access to this sector requires a certain amount of expertise, which limits the risks of exposure to uninformed customers. The legislation does not provide for an assessment

of the fit-and-proper nature of institutional SICs[38] and small alternative OPCAs. Particular attention should be paid to small alternative OPCAs. Although they are relatively uncommon and account for only a marginal proportion of assets under management (around EUR 8.3 billion), the regulatory framework applied to them remains partially deficient. This is because the FSMA lacks the authority to verify some of the conditions under which these entities access the market and conduct their business. Overall, despite the very significant financial weight it carries, the asset management sector is classified as moderately important in terms of AML/CFT materiality, due to the concentration of risks in a minority of players and a generally well-informed clientele.

91. **Bpost** is a sui generis entity under public law, offering both postal services and financial services, such as payments into third-party accounts and "bpaid" prepaid cards. It also acts as an agent for payment institutions authorised in another EU Member State. Income from postal financial products accounts for only a very small proportion of its business. Bpost's customers are exclusively natural persons acting for personal purposes, and their operations are limited to Belgian territory. The 2015 MER had recommended the implementation of AML/CFT supervision of Bpost. Since 2016, this supervision has been carried out by the Treasury (SPF Finance). The ML/TF risks associated with Bpost's activities are reduced by their geographical limitation to Belgium, but the possibility of withdrawing funds loaded onto "bpaid" cards abroad introduces a risk factor. Bpost's financial services, although declining, remain sensitive due to the predominance of cash and the relative anonymity associated with "bpaid" cards. Consequently, despite a current decline in business volumes, these products retain a certain materiality and Bpost is considered as being of moderate importance.

Low importance

92. **Portfolio management and investment advisory companies** – This sector comprises 35 entities, whose activities primarily involve portfolio management, investment advice and cross-border transactions, often on behalf of wealthy or institutional clients. These entities are strictly regulated by the FSMA. ML/TF risks are moderate to high depending on the customer profile, the products offered and the use of digital channels, which may complicate the verification of identity. This sector is therefore classified as being of low materiality in terms of AML/CFT, due to its limited weighting, robust regulations and generally controlled risks.

93. **Central security depositories** – Central security depositories are subject to AML/CFT obligations under the supervision of the BNB. Given the nature of their activities and the stringent regulatory framework, the ML/TF risks are considered low.

94. **Finance leasing and leasing companies** – Leasing is a professional financing activity, mainly used for vehicles and immovable equipment and facilities. The main risks relate to movable property leasing, especially the acquisition of luxury vehicles through dubious financial arrangements. However, immovable property leasing is moderately vulnerable and poses a relatively low threat.

95. **Independent financial planners** – There are very few representatives of this sector, with only five registered professionals, who offer a general financial advice service without issuing recommendations on specific investments or intervening in actual financial transactions. No cases of ML or TF involving this profession have been reported. The financial volumes involved are also very limited. This sector is therefore classified as being of low materiality vis-à-vis AML/CFT.

96. **Mutual guarantee companies** – This sector has a very small balance sheet. This is not a stand-alone activity: mutual guarantee companies' operations are always carried out as part of a pre-existing

[38] Except for institutional SICs, which are also approved lenders.

relationship between the customer and a credit institution. This sector is therefore classified as being of low materiality vis-à-vis AML/CFT.

DNFBPs

Main characteristics and weighting of designated non-financial businesses and professions (DNFBPs)

97. **Casinos and gaming operators** – Belgium has 9 licensed casinos (class I), authorised to offer their games online. In 2022, Gross Gaming Revenue (GGR) amounted to EUR 593 million (EUR 139 million physical and EUR 454 million online).

98. **Company service providers** – For AML/CFT obligations, the sector in Belgium only includes business centres (see R.22 TC Annex and IO.1). There were approximately 664 operators in 2023. These entities provide domiciliation, secretarial and administrative services for 40,000 to 50,000 companies.

99. **Estate agents** – In January 2023, 10,438 agents were registered with the Belgian Professional Institute of Estate Agents (*Institut Professionnel des Agents Immobiliers – IPI*). This sector operates within a large-scale property market (nearly EUR 1,872 billion in assets). Estate agents frequently participate in sales, rental and management transactions.

100. **Diamond dealers** – In 2023, 1,390 companies were registered with SPF Economy, concentrated mainly in the city of Antwerp, and had an annual trading volume of EUR 22.54 billion.[39] This sector has seen a significant drop in activity in recent years, mainly due to the effects of international sanctions on diamonds of certain origins and competition from the synthetic diamond market.[40] The diamond-trading entities based in Belgium participate mainly in diamond trading, cutting and distribution. The diamond sector accounts for 3% of Belgium's total trade and is its second largest export by value. In 2024, the average daily trading value amounted to EUR 102 million.[41]

101. **Notaries** – At the end of 2023, 1,758 notaries were operating in 1,106 practices nationwide, serving as public officials in a limited number of offices, and intervening in procedures with major legal and property implications, such as real estate sales, gifts and inheritances. Notaries in Belgium are public officials appointed by the King. They carry out this public function in a self-employed capacity.[42]

102. **Statutory auditors** – Belgium has 847 individual auditors and 699 licensed firms. In 2022, some 15,000 assignments were carried out, representing almost 67.5% of sector sales of EUR 750 million. Statutory audit activities, overseen by the Audit Oversight Board (*Collège de supervision*), involve a high level of responsibility. In Belgium, there are two categories of statutory auditors: PIE auditors, who audit public interest entities (PIEs), and non-PIE auditors, who audit other entities.

103. **Chartered accountants –** This segment has around 14,200 members and over 9,000 firms, with an estimated annual turnover of EUR 2.3 billion. The bulk of the business is based on accounting and tax compliance assignments, mainly for SMEs.

104. **Lawyers** – Belgium has more than 19,000 lawyers, who belong to the Order of the French-speaking and German-speaking bars, and *De Orde van Vlaamse balies*, plus the Bar to the Court of Cassation. In the French-speaking and German-speaking Bars, 6.4% of lawyers declared company law and the law of legal persons as their main activity in 2022 (14% as their secondary activity).[43] In Brussels, private customers account for less than half of revenue, whereas in other districts this proportion can rise to 70%.

---

[39] Antwerp World Diamond Centre (AWDC), Facts & Figures 2024, AWDC, Antwerp, 2024, https://www.awdc.be/facts-and-figures

[40] Antwerp Diamond Industry Data | AWDC

[41] Antwerp World Diamond Centre (AWDC), Facts & Figures 2024, AWDC, Antwerp, 2024, https://www.awdc.be/facts-and-figures

[42] The notary - Notaire.be

[43] Barometer survey of French- and German-speaking Belgian lawyers

105. **Bailiffs** - In 2024, 599 bailiffs were operating out of 212 offices nationwide. Bailiffs are involved in serving documents, enforcing court decisions and collecting debts, including in civil and commercial disputes.

Table 0.3. Designated non-financial businesses and professions

Obliged entity/sector	Number of entities	Balance sheet/ outstanding/ issued 2024 (EUR)	AML/CFT supervisory authority[44]
Casinos (Art. 5, §1, 33°)	9 (online and offline assets)	GGR: EUR 0.594 billion[45]	Belgian Gaming Commission (SPF Justice)
Company service providers[46] ("business centres") (Art. 5, §1, 29°)	664 (including 523 for domiciliation)	Number of companies hosted: between 40 000 and 50 000	SPF Economy (since 2018)
Real estate agents (Art. 5, §1, 30°)	10 438	Belgians' property assets: EUR 1,872 billion	SPF Economy
Diamond dealers[47] (Art. 5, §1, 31°)	1 390	Imports (2023): EUR 15.1 billion Exports: EUR 15 billion	SPF Economy
Certified chartered accountants (Art. 5, §1, 24°-25°)	10 176[48]	Sector revenue: 2.3 billion	Institute for Tax Advisors and Accountants (ITAA)
Statutory auditors *(réviseurs d'entreprise)* (Art. 5, §1, 23°)	1 990[49]	Income: 0.76 billion	Audit Oversight Board (*Collège de supervision des réviseurs d'entreprises*)
Lawyers (Art. 5, §1, 28°)	19 300	Maximum of 1.3% of GDP[50]	President of the Bar
Notaries (Art. 5, §1, 26°)	1 758	Total sector revenue: EUR 1.8 billion *(0.2% of GDP)*	National Chamber of Notaries (*Chambre Nationale des Notaires*)
Bailiffs (Art. 5, §1, 27°)	599	Total sector revenue: EUR 0.27 billion *(0.046% of GDP)*	National Chamber of Bailiffs (*Chambre nationale des huissiers de justice*)

Source: Belgian authorities

[44] List of supervisory authorities: see Art. 85 of the Belgian AML Law

[45] Gross Gaming Revenue is the difference between the initial total amount wagered and the total amount paid out as winnings: 139 million offline and 454 million online.

[46] Head office suppliers only. This decision was taken on the basis of a risk analysis and is explained at length in the explanatory memorandum to the Law of 29 March 2018 (see p. 6, point 2 and pp. 10 to 21).

[47] Prohibits all cash transactions over EUR 3,000 in general and introduces even more restrictive rules for the sale of precious materials, scrap metals and copper cables.

[48] Figures - concerning economic professionals acting independently (not those on employment contracts) – taken from the ITAA's 2024 annual report: 4,804 tax accountants (+347 trainees), 3,866 certified chartered accountants (+500 trainees) and 634 certified tax advisers (+25 trainees), 3,350 certified chartered accountant firms, 3,594 tax accountant firms, 465 certified tax adviser firms, 2 firms of certified chartered accountant trainees and 1,670 unspecified firms.

[49] 847 natural person statutory auditors; 451 trainee statutory auditors; 699 legal person statutory auditors and two third-country auditors.

[50] There are no figures for Belgium as a whole. However, a study by the Brussels Bar (Observatory of the Legal Profession | AVOCATS.BE) indicates that the economic weight of its members (Dutch-speaking and French-speaking lawyers combined) is equivalent to at least 1.3% of the GDP of the Brussels-Capital Region. This percentage is likely to be lower in the other local Bars and consequently, this figure of 1.3% (which is a minimum for the Brussels-Capital Region) represents a maximum figure for Belgium as a whole.

Materiality

106. The evaluation team applied the following weightings to assess the implementation of preventive measures by DNFBPs: *very great importance* for diamond dealers; *great importance* for business centres,[51] estate agents, chartered accountants, notaries and casinos; *moderate importance* for lawyers; and *low importance* for other DNFBPs.

Very great importance

107. **Diamond dealers** – Belgium is a major player in the diamond trade, which is mainly concentrated in Antwerp. Internationally, this sector is highly exposed to money laundering and tax evasion risks, due to the lack of transparency in some countries regarding the origin and valuation of diamonds, the emergence of alternative distribution channels and the frequent use of international organisations to optimise transactions for tax purposes, falsify goods and certificates, deliberately conceal the identity of the actual buyers or sellers and disguise the origin of funds. The characteristics of diamonds may also be similar to cash. Diamond prices may fluctuate according to a number of factors, including demand, transfer prices (a set of rules for setting prices between affiliated companies) and targeted sanctions imposed by the European Union. The value of diamonds can also be underestimated or overestimated, which facilitates the injection of funds of dubious origin into the legal economy. In recent years, the sector in Belgium has come under pressure from sanctions affecting certain diamond-exporting countries, leading to a 38% drop in imports and highlighting the links between Antwerp, ALROSA (the world's leading diamond producer) and Russian companies involved in mining in the Central African Republic. In addition, the low number of STRs (one in 2024) indicates a lack of vigilance or knowledge of AML/CFT obligations among diamond dealers. This sector remains highly vulnerable, which justifies its classification as a sector of the greatest importance in terms of AML/CFT risk.

Great importance

108. **Company service providers** ("business centres") - In Belgium, only domiciliation services (i.e. the provision of head offices), have been subject to AML/CFT obligations since the entry into force of the Law of 29 March 2018 (see R.22 in the TC Annex and IO.1). These entities are usually small companies with a limited AML/CFT culture. The ML NRA indicates a moderate level of risk for this sector, due to the limited scope of the services offered. Some of these services are offered remotely, which complicates the monitoring of the actual beneficial owners. In addition, CTIF has observed the use of business centres in ML schemes, either voluntarily or as a result of abuses in cases involving shell companies with fictitious directors, fictitious head offices and vague corporate purposes, which complicate the identification of beneficial owners and the traceability of illicit transactions. Supervisors have a sound understanding of the risks associated with the sector, but many small business centres still operate illegally, without being registered.

109. **Estate agents** – The Belgian real estate market, which expanded between 2012 and 2022, has stabilised and even appears to have contracted between 2022 and 2024.[52] In the majority of transactions, the preliminary sales agreement is drawn up by a notary and signed by the parties without the involvement of an estate agent. In the NRA, the property sector in general is considered as posing a significant ML risk, due to certain specific methods in particular, such as the use of mortgage loans, cross-selling and fictitious leases. Several vulnerabilities have been identified by the authorities and the CTIF in particular, including

[51] In the company service provider category, only domiciliation or business centre services (i.e. the provision of head offices) are subject to the AML/CFT regime (see R.22 in the TC Annex).

[52] A dwelling house cost an average of EUR 329,743 in 2024, up 2.2% compared with 2023 (EUR 322,780) – Immobilier : diminution des ventes - Fednot; Real estate prices | Statbel

property purchases purchased with illicit funds, and the deliberate under- or over-estimation of prices. Because of these factors, the real estate sector is classified as being of great importance.

110. **Chartered accountants** – The ML NRA indicates a moderate level of risk for this sector. Although the number of incidents detected involving chartered accountants is not very high, some professionals have been involved, voluntarily or involuntarily, in ML schemes. Chartered accountants play a key role in businesses, notably by participating in company creation and management, helping their clients to draw up financial plans, and overseeing company accounts. They may also propose their own business addresses as domiciliation addresses for companies that may turn out to be criminal. Investigations by the Federal Police Criminal Investigation Department (*Police Judiciaire Fédérale* – PJF) reveal that sophisticated criminals occasionally work with respected law firms, which reinforces their ability to operate under the guise of legitimacy. Despite strict supervision by the authorities, the risks remain high.

111. **Notaries** – These professionals play a central role in sensitive transactions such as the incorporation of companies – with around 3,500 companies created every month – and foundations. They are actively involved in property transactions, in which recourse to their services is mandatory. This strategic position exposes them to the risk of involvement – voluntarily or involuntarily – in ML operations. Some cases have shown that certain notaries have been used by criminals and have therefore, whether voluntarily or involuntarily, facilitated such practices, notably by creating fictitious companies used for serious tax and social security fraud, as in the Brazilian network (see R.I7). Because of these vulnerabilities and the involvement of notaries in the real estate sector, which is considered high-risk by the assessors, the notarial sector is considered to be highly exposed to ML/TF risks.

112. **Casinos** – Belgian law stipulates that the nine licensed physical casinos have the exclusive authority to operate online casinos. As a result, these operators run 58 casino websites and 22 additional betting websites. Although the regulations impose a limit of EUR 3,000 on cash transactions and physical casinos prohibit both inter-account transactions and current accounts for customers, ML vulnerabilities still exist. The ML NRA considers the leisure sector as posing a significant risk, but the assessment of the risk levels of the various casinos remains unclear, especially due to the differences in the establishments' sizes and incomes. Furthermore, the effectiveness of AML/CFT supervision in this sector is uncertain, as the Gaming Commission (*Commission des Jeux de Hasard*) is unable to carry out appropriate supervision due to a lack of staff (see IO.4).

Moderate importance

113. **Lawyers** – Although not mandatory for the creation of companies, lawyers' services are sometimes used for this purpose. Their main contribution to the creation of a company or an association, is to advise their clients on the choices to be made (legal form, shareholders' agreement, etc.) and to assist them in implementing their choices (e.g. formalities with the Banque-Carrefour des Entreprises, i.e. the legal persons national register, see below). They participate in asset management, or in real estate and financial transactions. More rarely, they may also be involved in setting up foreign trusts and *fiducies* (as trusts and *fiducies* are legal arrangements that are not provided for under Belgian law and cannot be set up in Belgium – see below). The CTIF has identified cases in which tax lawyers are alleged to have facilitated tax fraud and money laundering and where certain lawyers have been identified as having deliberately provided money laundering services, notably for criminals involved in drug trafficking or financial fraud. The main vulnerabilities in the sector include the holding of third-party funds in "*comptes de qualité*" (undesignated accounts exclusively reserved for handling customers' or third-party funds) and the use of these accounts to carry out international transfers, for which enhanced and automatic supervision measures have recently been introduced (see IO.4). The ML NRA assigns a moderate level of risk to lawyers.

Low importance

114. **Statutory auditors** – These professionals do not appear to be directly involved in fraudulent transactions, as their role tends to focus on compliance and financial certification. The Belgian Institute of Statutory Auditors (*Institut des Réviseurs d'Entreprises – IRE*), which is responsible for maintaining the register and granting access to the profession, applies rigorous approval procedures, but the lack of transparency in checks on the conditions of access to the profession and the absence of closer monitoring of statutory auditors on the register, especially non-PIE auditors, may create loopholes, albeit of a minor nature, that could be exploited by criminals.

115. **Dealers in precious metals and stones** - In Belgium, cash payments in excess of EUR 3,000 are prohibited, which puts this sector below the thresholds set by the FATF and excludes them from the obligation to implement preventive measures. As a result, a low level of risk has been assigned to this sector. However, the use of cash is still common in the precious metal- (gold-) purchasing, luxury goods and scrap metal recovery businesses, which raises the need for the effective monitoring of this limit.

116. **Bailiffs -** Bailiffs have a limited scope of intervention and their material importance remains low in the analysis of AML/CFT materiality. However, when enforcing court rulings, bailiffs may be confronted with high-risk situations. One example of this is when a debtor in default of payment (especially for VAT or social security debts) offers to pay a large amount in cash – which may be an indication of money laundering, particularly in connection with fraudulent bankruptcy or misuse of corporate assets. This sector is therefore classified as being of low materiality for AML/CFT purposes, due to its limited weighting, the regulated nature of its activities and the rarity of risky situations.

Legal persons and arrangements

117. The **private limited company** (*société à responsabilité limitée* – SRL) is the most common legal form, accounting for just over 60% of all legal persons registered with the Banque-Carrefour des Entreprises (the national register containing basic information on legal persons). The number of new SRLs being created has risen steadily since the Belgian Code of Companies and Associations (*Code des sociétés et des associations* – CSA) came into force, from 2,111 per month in 2019 to 3,401 per month in 2023. SRLs are the most frequently identified legal form in suspected ML cases and investigations, accounting for 75% of the legal persons identified in the CTIF's reports to the judicial authorities and 30% of ML investigations launched between 2019 and 2023. Around 12% of SRLs are owned by at least one (Belgian or foreign) legal person or by a legal arrangement.

118. **Non-profit organisations** (NPOs) (*associations sans but lucratif* – ASBL) are the second most common legal form, representing almost 15% of existing entities. The number of new ASBLs being created has risen steadily since the CSA came into force: 134,000 per month in 2021 and around 144,500 per month in early 2024. Around 6% of ABSLs are owned by at least one legal person (Belgian or foreign) or by a legal arrangement.

119. **Public limited companies** (*sociétés anonymes* – SA) account for 10% of all legal persons operating in Belgium and 9% of the cases referred by the CTIF to the judicial authorities. Around 11% of SAs are owned by at least one legal person (Belgian or foreign) or by a legal arrangement.

120. The table below presents the different types of legal person that can be created in Belgium and their main characteristics. All these legal persons must be registered in the Banque-Carrefour des Entreprises register, which is maintained by the commercial court registrars.

Table 0.4. Legal persons

Type of legal persons	Number of registered entities	Applicable laws / regulations / requirements [53] Other information (e.g., substantial changes, etc.)
Company or association without legal personality	2 6374	Art. 1.5 CSA De facto association (CSA - Art 1:5, §1) Registration with the Banque-Carrefour des Entreprises may be required in certain cases, and particularly when the association carries out an activity subject to VAT or employs salaried workers; An ordinary limited partnership (*société simple*) (CSA - Art 1:5,§1), used mainly for asset management and estate planning, is the only type of company without legal personality. If the partners decide to assign legal personality to their ordinary limited partnership, it may take the form of a general partnership (*société en nom collectif* – SNC) or a limited partnership (*société en commandite* – SComm).
Limited liability company (*société à responsabilité limitée* – SRL)	576 107	*Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 The preferred form of company for small and medium-sized enterprises in Belgium, having replaced the former SPRL, SPRL Starter and SPRLU since 1st May 2019.
Public limited companies (SA)	95 313	*Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 Legal form often chosen by medium-sized and large companies that generate significant revenues.
Limited partnership (*société en commandite* – SComm)	58 315	*Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 Brings together partners with unlimited liability and limited partners. The partners with unlimited liability are responsible for management, while the limited partners are financial backers who cannot intervene in management.
General partnerships (Société en nom collectif - SNC)	29 334	*Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 Company incorporated by jointly and severally by partners who have unlimited liability for the company's commitments.
Cooperative company (*société coopérative* – SC)	20 519	*Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 Since the reform of the CSA, only one type of cooperative company can be created (thirteen types previously existed). Its main objective is to satisfy the needs of shareholders and/or to develop their economic or social activities.
European Economic Interest Grouping (EEIG)	268	European Regulation No 2137/85 on operating procedures and incorporation. *Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 The objective of an EEIG is to facilitate or develop its members' economic activities by pooling resources, activities and expertise in order to achieve better results than by acting in isolation. It and may not include the members' own activities. The EEIG's activities must be related to and ancillary to its members' economic activities.
European company (*Société européenne* – SE)	12	European Regulation No 2157/2001 on operating procedures and incorporation. *Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 The SE offers a company the opportunity to carry out its activities in various European Union countries under a single, harmonised statute.
European cooperative society (*Société coopérative européenne* – SCE)	7	European Regulation No 1435/2003 on operating procedures and incorporation. *Incorporation formalities*: CSA – Art. 2:5 to 2:8 *Information to be published in the* Moniteur belge: CSA – Art. 2:14 Optional legal form of cooperative intended to facilitate the cross-border and transnational activities of cooperatives. To be incorporated, an SCE's members (natural or legal persons) must be resident in more than one European Union country.
Non-profit organisations	139 276	*Incorporation formalities*: CSA – Art. 2:5 to 2:7 and 2:9 *Information to be published in the* Moniteur belge: CSA – Art. 2:15

[53] Laws and regulations applicable to all types of legal persons and arrangements (unless otherwise stated in the table) :

- The obligation to collect and record data on beneficial owners: UBO Royal Decree Art. 3 for all legal entities and the UBO Royal Decree Art. 4 for legal arrangements.
- The obligation to collect and update information on beneficial owners: Belgian Code of Companies and Associations (CSA) – Art. 1: 35.
- Compulsory registration with the Banque-Carrefour des Entreprises: Belgian Code of Economic Law (CDE), Art III.16 to III.57.

Type of legal persons	Number of registered entities	Applicable laws / regulations / requirements [53] Other information (e.g., substantial changes, etc.)
(NPOs)		Grouping of at least two individuals or legal entities (instead of three previously) whose main objective is the pursuit of a not-for-profit purpose. Although their main purpose is social, ASBLs may also carry out economic activities, provided that the profits obtained are used exclusively to achieve the non-profit object defined in the ASBLs' articles of association. They are therefore prohibited from directly or indirectly distributing or procuring any financial benefit whatsoever to their founders, members, directors or any other person, except in the context of the not-for-profit purpose set out in the Articles of Association.
International non-profit organisation (*Association internationale sans but lucratif* – AISBL)	2 435	*Incorporation formalities*: CSA – Art. 2:5 to 2:7 and 02:10 *Information to be published in the* Moniteur belge: CSA – Art. 2:16 An association dedicated to supporting public-interest objectives on an international scale. To obtain legal recognition, it must demonstrate its commitment to objectives of international interest in its articles of association.
Private foundation (Fondation privée – FP) [54]	2 106	*Incorporation formalities*: CSA – Art. 2:5 to 2:7 and 02:11 *Information to be published in the* Moniteur belge: CSA – Art. 2:17 A legal person with no members, whose assets are allocated to the pursuit of a public-interest aim the context of one or more specific activities that constitute its purpose. A foundation may also carry out economic activities, provided that the profits obtained are used exclusively to achieve the purpose of the foundation and are not distributed to its founders or directors.
Public interest foundation (*Fondation d'utilité publique* – FUP)	668	*Incorporation formalities*: CSA – Art. 2:5 to 2:7 and 02:11 *Information to be published in the* Moniteur belge: CSA – Art. 2:17 A foundation may be recognised as being in the public interest if its purpose is to carry out work of a philanthropic, philosophical, religious, scientific, artistic, educational or cultural nature.
Foreign entities	7 362 [55]	*Formalities for opening a branch*: CSA – Art. 2:24 to 2:26 All foreign entities with a branch or a site unit in Belgium are registered with the Banque-Carrefour des Entreprises under the legal title of "foreign entity".
Trusts, *fiducies*	724 [56]	Belgian Code of Private International Law (*Code de droit international privé*) of 16 July 2004 (Chapter XII) on their validity Trusts, *fiducies* and similar foreign legal arrangements.

121. Belgian law does not allow for the creation of trusts or similar legal arrangements. Belgium has not ratified the Hague Convention of 1st July 1985 on the Law Applicable to Trusts and on their Recognition. However, the Belgian Code of Private International Law (Chapter XII) recognises the validity of trusts established in Belgium and incorporated under foreign law. Belgium also applies the requirements of Recommendation 25 to trusts and similar arrangements managed from Belgium (See TC Annex).

122. Belgium identifies a total of 66 012 foreign entities with a link to the country, 7 645 of which have a branch or a site unit in Belgium. The other entities are subject to various Belgian legal obligations, such as carrying out activities subject to VAT, employment subject to Belgian social security, participation in public contracts, or the leasing of real estate in Belgium. These entities must register with the Banque-Carrefour des Entreprises and declare their beneficial owners to the UBO register.

[54] Recognition of the legal forms of foundations: CSA – Art. 1:7.

[55] Subsidiaries of foreign entities established in Belgium adopt the legal form of a company or legal person under Belgian law, and are therefore not included in the number of foreign entities registered.

[56] This number corresponds to the number of trusts and other similar legal arrangements recorded in the UBO register as an intermediate entity that has effective control over a Belgian legal entity.

Structural elements

123. The structural elements needed to ensure an effective AML/CFT system are present in Belgium. Belgium possesses stable institutions which are held accountable. It is a state governed by the rule of law, with a competent and independent judiciary.

124. There is a high-level political commitment to fighting crime, particularly drug trafficking and organised crime. With its institutional structure, Belgium has the necessary framework to ensure the implementation of its AML/CFT system. Responsibility for developing and implementing the AML/CFT policy in Belgium is shared between the competent authorities with clearly defined statuses and roles (seethe introduction).

125. However, some important strategic AML/CFT decisions appear to have been delayed in the absence of a fully functioning government (see Chap. 2), and the investigating and prosecuting authorities appear to be confronted with recurrent resource problems (see Chap. 3).

126. As a member of the EU, Belgium is bound by EU law. EU Regulations apply directly and in their entirety in Belgium. EU Directives, which are also binding as to the results to be achieved, are transposed through domestic law.

Other contextual factors

127. Belgium is an open, predominantly service-oriented economy at the heart of the Eurozone, with flows of goods and commodities into and out of the country that are well above the average for other EU countries.[57] It occupies a strategic geographical position in Europe, with the port of Antwerp-Bruges serving as its main point of entry and an international logistics hub, and intra-Community borders shared with France, Germany, Luxembourg and the Netherlands. Belgium is also home to the headquarters of major European and international organisations such as the EU and the North Atlantic Treaty Organisation (NATO). These characteristics expose the country to significant financial and non-financial flows, which may be conducive to the development of criminal phenomena. Furthermore, Belgium has a high level of tax and social charges within the EU,[58] which tends to encourage fraud.

AML/CFT/CPF strategy

128. As regards ML, the 2023 ML NRA led to the adoption of an AML Action Plan in March 2024 by the Ministerial Committee for Coordinating Measures Against Laundering Money from Illegal Sources (*Comité ministériel de coordination de la lutte contre le blanchiment de capitaux d'origine illicite*). This Ministerial committee is the national AML coordination platform (see section below). The AML Action Plan defines four guidelines for national AML/CFT policy – strengthen and monitor compliance with preventive measures; increase the transparency of legal structures and arrangements; reinforce detection and prosecution; optimise coordination and international cooperation. It sets out concrete recommendations to be implemented by the competent authorities in each of the four areas (see IO.1).

129. With regard to TF, there is no standalone strategy, but the reference framework is the Terrorism, Extremism and Radicalism Strategy (TER Strategy) adopted in 2021, replacing "Plan R" and enhanced by the lessons learned from the attacks of 2015 and 2016.[59] The Belgian authorities have demonstrated the existence of an operational counter-terrorism-financing strategy, which was primarily drawn up following

[57] SPF Economy: Overview of economic activity in Belgium [in French]

[58] OECD – Tax wedge

[59] 54K1752010.indd

the 2016 attacks and is based on the strong, multidisciplinary integration of counter-terrorism and CFT measures (see IO.1 and 9).

130. As far as proliferation financing is concerned, there is no targeted CPF strategy. The 2021 National Security Strategy addresses counter-proliferation issues, but does not address the issue of their financing.

Institutional and legal framework

Institutional framework

Coordination bodies

131. The **Ministerial Committee for coordinating measures against laundering money from illegal sources (Ministerial ML Committee)** is responsible for establishing general AML policy. It is chaired by the Minister for Justice and its members are the Ministers for Finance, Interior, Economy and Small and Medium-sized Enterprises. It is assisted by a technical body – the AML Coordination College (*Collège de coordination de la LBC d'origine illicite*) – co-chaired by the President of the CTIF and the Prosecutor General, which oversees the implementation of general AML policy and the AML priorities. The College for AML coordination brings together:

- the Partners' Assembly, chaired by the CTIF, which coordinates the ML risk analysis. Its members are representatives of the National Bank of Belgium (*Banque nationale de Belgique*, BNB), the Financial Services and Markets Authority (FSMA), the Federal Public Services (*Services publics fédéraux* – SPF) for Finance, Economy and Justice, the College of Prosecutors General, the Federal Police and the Standing Committee of the Local Police.
- the judicial platform, chaired by the Prosecutor General, which coordinates the tasks and activities of the criminal justice authorities in terms of law enforcement and ML. Its members are representatives of the Prosecutors General, the Federal Public Prosecutor, the Council of King's Prosecutors, the Council of Labour Auditors, the Federal Police, the Standing Committee of the Local Police and the Directorate-General for Legislation and Fundamental Freedoms and Rights of SPF Justice.

132. The **National Security Council (*Conseil national de sécurité* – CNS**) is responsible for overall intelligence and security policy in the country, including the strategic coordination of measures to counter terrorism and TF. The CNS also oversees the strategic coordination of measures to counter proliferation and PF. It is chaired by the Prime Minister and its members are the Ministers of Justice, Defence, the Interior, Foreign Affairs and the Deputy Prime Ministers. The CNS is assisted by:

- a political body – the Strategic Committee (Intelligence and Security) – which prepares for the CNS meetings and ensures the coordinated implementation of its decisions. The committee members are representatives of the Prime Minister and other members of the government who are members of the CNS.
- a technical body – the Coordination Committee (Intelligence and Security) – which ensures coordination, collaboration and exchanges of information between members. The standing members are the General Administrator of State Security, the Head of the General Intelligence and Security Service of the Armed Forces, the Director of the Threat Analysis Coordination Body (*Organe de coordination pour l'analyse de la menace*), the Commissioner General of the Federal Police, the Director General of the Directorate General for the National Crisis Centre of the Federal Public Service Home Affairs, the Chair of the Management Committee of SPF Foreign Affairs, Foreign Trade and Development Cooperation, a representative of the College of Prosecutors General, the Federal Prosecutor, the Head of Defence and the Director of the Belgian Centre for Cybersecurity.

The President of the CTIF is one of the non-standing members who may be invited to take part in the Coordination Committee.

Financial information

133. The Cellule de Traitement des Informations Financières (CTIF) is the independent Belgian financial intelligence unit (FIU) responsible for receiving, analysing and disseminating suspicious transaction reports relating to ML and TF (see R.29 in the TC Annex). It provides the link between the prevention and law enforcement aspects of the AML/CFT system. It is chaired by a judge and includes legal, financial and police experts. The CTIF Bureau, consisting of a presiding judge and specialist members from the financial, judicial and police sectors, decides on a collegial basis whether cases should be referred to the competent authorities when there is serious indications of ML/TF.

134. The Customs service within the General Customs and Excise Administration (Administration générale des douanes et accises – AGDA) oversees the incoming and outgoing cross-border transportation of cash, securities and valuables. It does not have investigative powers: the public prosecutor's office and the CTIF have the authority to investigate suspected cases of ML/TF (see R.32 in the TC Annex).

135. The Anti-Fraud Unit (Cellule anti-fraude – CAF) at SPF Finance ensures cooperation between agencies which are directly or indirectly responsible for combating the different types of fraud (Public Prosecutor's Office, SPF Economy, SPF Foreign Affairs, CTIF, Federal Police (DJSoc), OLAF, etc.).

136. The various inspection services of the institutions responsible for social security (e.g. ONSS, INASTI) carry out administrative checks on compliance with the various social regulations. They do not have investigative powers: the Labour Prosecution Services ("Auditorats du travail") have the authority to investigate suspected cases of social fraud and associated ML/TF.

Investigations and prosecutions

137. The **College of Prosecutors General** sets criminal law guidelines in AML/CFT matters. At police level, the Directorate General of the Federal Police Criminal Investigation Department draws up the framework for ML/TF investigations and predicate offences.

138. Responsibility for investigating and prosecuting ML offences is shared between the Public Prosecutors' Offices within the judicial districts and the Federal Prosecutor's Office. ML investigations are mainly conducted by the Public Prosecutors' Offices in Antwerp and Brussels, where specialised judges are assigned to the ECOFIN unit. The other Public Prosecutors' Offices also have ECOFIN units, but with more limited resources. The Federal Public Prosecutor's Office handles a limited number [60] of ML cases, which it investigates on its own initiative. The judges within the "*Auditorats du travail*" have the authority for cases of social security fraud linked to ML.

139. With regard to TF, the Federal Public Prosecutor's Office has exclusive de facto jurisdiction to investigate and prosecute terrorist financing.

140. Local and federal prosecutors rely mainly on specialist investigators within the Federal Police Criminal Investigation Department to conduct ML/TF investigations and investigations into predicate offences. These investigators are assigned to ECOFIN departments in 14 local investigation units (Federal Police Criminal Investigation Departments – PJFs). TF cases are only investigated by the five local PJFs specialising in countering terrorism and the financing of terrorism. When an investigation is opened, it is led by a "*juge d'instruction*" (investigating judge).

[60] Two cases were being investigated and three cases were at the procedural regulation stage in February 2025.

141. **The Central Office for Seizure and Confiscation (*Organe central pour la saisie et la confiscation* – OCSC)**, set up in 2003, is the specialised agency responsible for the management of sums seized in criminal proceedings in Belgium (cash, accounts with financial institutions, etc.) and the valuation of seized assets. The management of virtual assets was also entrusted to the OCSC in 2018. Successive laws passed in 2018 and 2024[61] have improved its functioning and it is also governed by a circular from the College of Prosecutors General.[62] The OCSC has a staff of 45 people, including four federal police liaison officers and two liaison judges seconded to the OCSC on a full-time basis.

142. The OCSC's legal remit also includes the enforcement of judicial confiscation orders and the provision of training and operational support for law enforcement authorities, particularly in the preparation of requests for mutual legal assistance.

Other authorities

143. With regard to targeted financial sanctions (TF and PF), **SPF Finance/Treasury** is the competent authority for implementing asset-freezing measures and also monitors compliance with the obligations of reporting entities. For each new designation, all persons concerned are required to notify SPF Finance whether or not they hold funds on behalf of the targeted persons and entities. For their part, the AML/CFT supervisory authorities of FIs and DNFBPs are responsible for ensuring that reporting entities have developed and apply effective internal control procedures and measures to comply with TFS-related obligations.

Supervisory authorities

Financial sector

144. The **National Bank of Belgium (BNB)** is responsible for the AML/CFT supervision of financial institutions (FIs) subject to its licensing or prudential supervision. These includes credit institutions (banks), payment and electronic money institutions, and insurance companies (see table0.1).

145. The **Financial Services and Markets Authority (FSMA)** is responsible for the AML/CFT supervision of investment firms, fund managers, "non-exclusive" insurance intermediaries operating in the life insurance sector, brokers in banking and investment services, bureaux de change, independent financial planners, consumer credit and mortgage lenders,[63] and market operators (see table 0.1). It was formerly the AML/CFT supervisory authority for virtual asset service providers established in Belgium until the MiCA regulation came into force on 30 December 2024 (see IO.3).

146. **SPF Finance** is the competent authority for the AML/CFT supervision of Bpost's activities subject to the AML law, i.e. its activities related to postal financial services and electronic money issuance (see the Introduction).

Non-financial sector (DNFBP)

147. **SPF Economy** is responsible for the licensing and AML/CFT supervision of a number of non-financial sectors, including diamond dealers, company service providers and estate agents.[64] It also ensures compliance with the rules on limiting cash payments.

---

[61] Law of 4 February 2018 containing the missions and composition of the OCSC and the Law of 18 April 2024 on optimising the operation of the OCSC

[62] COL PG 09/2018

[63] However, the FSMA is not the AML/CFT supervisory authority for obliged entities subject to the AML/CFT supervisory authority of the BNB for the activities they carry out in their capacity as consumer credit and/or mortgage credit lenders.

[64] It also supervises sectors not covered by the FATF Recommendations (e.g. the arts and antiques sector).

148. AML/CFT supervision of the notarial profession is carried out by two levels of authority consisting exclusively of notaries: the ***Management Committee of the National Chamber*** (consisting of eight notary members), which sets the general rules of professional conduct and monitors the implementation of AML/CFT measures, and the eleven ***Provincial Chambers*** (consisting exclusively of notaries practising within the jurisdiction of the province), which are responsible for monitoring compliance with the rules of professional conduct at local level.

149. The **presidents of bars** are responsible for the supervision of lawyers, in their role as disciplinary authorities within each of the 19 bar associations, including Brussels, which is the largest. Each lawyer is affiliated to a specific bar but may have a secondary practice in a different one. The Brussels Bar is divided into two distinct linguistic orders (French and Dutch), each with its own president.

150. The **Institute for Tax Advisors and Accountants (ITAA)** is the AML/CFT supervisory authority for chartered accountants (and tax advisers) licensed in Belgium, and keeps a register of those authorised to practise.

151. The **Audit Oversight Board (*Collège de supervision des réviseurs* – CSR)** is the competent authority for the AML/CFT supervision of statutory auditors. The Institute of Statutory Auditors (*Institut des Réviseurs d'Entreprises* – IRE) is responsible for registration and licensing, which it carries out under a legal delegation, under the ultimate responsibility of the CSR.

152. The Belgian **Gaming Commission (*Commission des jeux de hasard* – CJH)** is responsible for the regulation and supervision of gambling, including casinos, gaming halls, betting agencies and cafés and bookshops offering games of chance.

153. The **National Chamber of Bailiffs** (*Chambre nationale des huissiers de justice*) is responsible for AML/CFT checks on bailiffs.

European bodies

154. At the Union's level, the relevant authorities with competence in AML/CFT are:

- The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) is a Union body entrusted with exercising direct supervision over certain financial institutions, ensuring convergence of supervision for the rest of the obliged entities, and coordination and support of EU FIUs;[65]
- The European Public Prosecutor's Office (EPPO) is responsible for investigating, prosecuting and bringing to judgment the perpetrators of, and accomplices to, criminal offences affecting the financial interests of the Union, including money laundering. In that respect, the EPPO undertakes investigations, carries out acts of prosecution and exercises the functions of prosecutor in the competent courts of the member states, until the case has been finally disposed of.

155. The European Central Bank (ECB) is the prudential banking supervisor in the Banking Union, working together with the prudential supervisory authorities of the participating member states within the 'Single Supervisory Mechanism' (SSM).[66] It is therefore another important actor in the institutional framework. While not an AML/CFT supervisor, the ECB carries out certain functions which are relevant both to AML/CFT and for prudential supervision purposes, such as granting or withdrawing licences for all credit institutions established in the Banking Union and carrying out suitability assessments of members of

[65] While AMLA was legally established in June 2024, it will commence carrying out its tasks progressively as of June 2025 (with direct supervision starting in 2028).

[66] The SSM refers to the system of banking supervision in the Banking Union. The Banking Union currently comprises 21 member states: the Euro Area member states and those other member states that establish close cooperation. The SSM itself comprises the ECB and the national supervisory authorities of the participating countries.

management bodies of significant credit institutions. In this context, the ECB cooperates with relevant AML/CFT authorities within the EU/EEA.

156. Other EU-level bodies and agencies have a supporting role, including Europol and Eurojust.

Legal framework

157. The AML/CFT legal framework in Belgium is based on national and European provisions. Legislative changes have been made to the legal framework since the FATF evaluation in 2015, notably to transpose European directives and other measures on AML/CFT.[67] The ML prevention system is now governed by the Law of 18 September 2017 (AML Law), which also implements the beneficial ownership register (UBO register).[68] The legal framework applicable to legal entities has also undergone significant changes with the entry into force of Belgium's new Companies and Associations Code (*Code des associations et des sociétés* – CSA) in May 2019. The CSA consolidates and replaces the former Companies Code of 1999 and the Associations and Foundations Law of 1921, and has led to an overhaul of corporate forms, which have been reduced to three main categories: companies, associations and foundations.

158. The main provisions on criminal justice matters are set out in the Criminal Code (*Code Pénal* – CP) and the Code of Criminal Procedure (*Code d'instruction criminelle* – CIC). These provisions have been supplemented by legislation. Since the 2015 MER, this includes the Law of 4 February 2018 reforming the Central Office for Seizure and Confiscation and the Act of 8 July 2018 extending access to the central point of contact for financial accounts and contracts. Belgium's criminal justice policy on ML is also laid down in circulars adopted by the College of Prosecutors General, including the "TRIM" Circular of September 2022 (see IO.7).[69] Regarding TF, the Circular of October 2024[70] lays down the formal framework for cooperation platforms on terrorism/TF (JIC/JDC, see IO.9).

Preventive measures

159. The AML/CFT Directive[71] sets out AML/CFT preventive rules, including the scope of obliged entities, provisions on the assessment of risks, CDD measures and record keeping requirements, beneficial ownership transparency requirements, reporting obligations, as well as the powers and tasks of FIUs and supervisors and information exchange and cooperation between authorities.[72] Traceability of fund and

[67] Including Directives (EU) 2015/849, 2018/843 and 2019/1153

[68] Several Royal Decrees have since been adopted to implement the law. For example, the operating procedures of the UBO register were specified by the Royal Decree of 30 July 2018 (RD July 2018).

[69] COL Circular 14/2022 of 29 September 2022

[70] COL Circular 16/2024 (confidential)

[71] Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (the "5th AML/CFT Directive").

[72] A new Regulation and Directive came into force (but not effect) on 9 July 2024 and Directive (EU) 2015/849 will be replaced as follows:

Regulation (EU) 2024/1624 (the "EU AML/CFT Regulation"), covers all preventive rules, including by setting out the scope of obliged entities and the rules that apply to their internal AML/CFT systems, CDD measures, record keeping requirements, reporting of suspicions to FIUs, as well as beneficial ownership transparency and mitigation of specific risks stemming from anonymous instruments such as bearer shares/share warrants, cash and anonymous accounts. The AML Regulation shall apply from 10 July 2027, except for certain provisions relating to professional football clubs and football agents which will apply on 10th July 2029.

Directive (EU) 2024/1640 (the '6th AML/CFT Directive') sets out the power and tasks of FIUs and supervisors and creates structures for cross-border cooperation and information exchange between authorities. It also includes provisions on the assessment of risks, including a direct obligation on the Commission to assess risks at Union level every 4 years (and more frequently as needed for specific risks) and on beneficial ownership registers, including directly applicable provisions regarding their interconnection. The 6th AML Directive shall be transposed by 10 July 2027, except for certain provisions related to: (i) access to Beneficial Ownership Registers which will have to be transposed earlier; and (ii) single access points to real estate data, which have a later transposition date.

crypto-asset transfers are regulated under Regulation (EU) 2023/1113 (the "Transfer of Funds Regulation" (TFR)).

160. The AML/CFT/CPF obligations of reporting entities are set out in Book II of the AML Law of 2017. Since 2015, certain sectors[73] have been added to the list of reporting entities. In May 2022, virtual asset service providers (VASPs), such as those engaged in trading between virtual money and fiat money or offering custodian and/or administration services for virtual assets or instruments enabling their supervision, have been included in the scope of AML/CFT measures.

161. In Belgium, dealers in precious metals and stones are not subject to AML/CFT obligations, as the law prohibits cash payments exceeding 3,000 euros (see R.22 in the TC Annex). Only diamond dealers are subject to these obligations, regardless of the payment method used.

162. With regard to company service providers, the scope of the AML Law of 2017 includes only one of the five categories of activities provided for by the FATF – providers of head offices for enterprises (business centres). SPF Economy is responsible for supervising this sector.

163. The BNB and FSMA Regulations meet the conditions of "Enforceable means" within the meaning of the note on the legal basis of the obligations of FIs and DNFBPs and VASPs.[74]

Supervisory arrangements

164. Title 4 of Book IV of the Belgian AML Law entrusts the supervisory authorities with the task of ensuring that reporting entities comply with their AML/CFT/CPF obligations.[75] The supervisory authorities in Belgium are listed below.

- For the financial sector: the National Bank of Belgium (BNB), the Financial Services and Markets Authority (FSMA) and the Federal Public Service for Finance (*Service public fédéral Finances* – SPF Finance) (see the Introduction and table 0.1 for a detailed description of their mandates).
- For the non-financial sector, the main competent authorities are the Federal Public Service for the Economy (SPF Economy), the Audit Oversight Board (*Collège de supervision des réviseurs d'entreprises* – CSR) and the Gaming Commission (*Commission des jeux de hasard* – CJH) (see the Introduction on the institutional framework).

165. Belgium also has several self-regulatory bodies (SRBs), designated by the AML Law as AML/CFT supervisory authorities. They are:

- Institute for Tax Advisors and Accountants (ITAA);
- Presidents of bars for lawyers;
- National and Provincial Chambers of Notaries;
- National Chamber of Bailiffs.

International cooperation

166. Because of its size and geographical location, Belgium is a gateway into the EU and Western Europe in general. The country is a trade crossroads and a transit country for people, goods, and services. It attracts significant financial and non-financial flows, which may fuel the development of criminal activities. The port of Antwerp-Bruges is central to both legal and illegal trade, particularly in narcotics. In addition, the financial sector is characterised by the presence of multinational financial groups and numerous financial

[73] Including professional football clubs (1st July 2021), art and antiques brokers (23 October 2021) and safe deposit box rental services (31st March 2024).

[74] Methodology p. 201

[75] Article 85 describes the distribution of these powers and the supervisory powers are defined in Articles 91 et seq.

service providers established in other EU Member States and operating in Belgium under the European passport.

167. The country is not characterised by a single profile in terms of illicit financial flows, due to the variety of criminal routes that cross it. It has the characteristics of a transit country for a large proportion of the flows associated with drug trafficking and tax and social security fraud, insofar as the proceeds of criminal activities do not seem to remain in Belgium. However, the offsetting technique is designed to reinject cash into Belgium, with the majority of large-scale operations involving transfers abroad. The commonality shared by these different scenarios is their significant connections with other countries, hence the importance of international cooperation for Belgium.

168. Belgium's neighbouring countries – the Netherlands, Germany, France and Luxembourg – are its main trading partners, and those with which it has the most highly developed international cooperation.

169. SPF Justice is the central authority in Belgium for mutual legal assistance (including for extradition). This agency handles incoming and outgoing cooperation requests from non-EU countries and is responsible for their management, quality, follow-up and confidentiality. This remit of SPF Justice is based on the numerous international conventions and bilateral agreements that Belgium has signed and ratified.[76] In the absence of such conventions or agreements, it may grant a request for mutual legal assistance based on the principle of reciprocity.

[76] The most recent include the Extradition Treaty and a Mutual Legal Assistance Treaty with the United Arab Emirates (2021), and the Extradition Treaty with China (2020).

1 Assessment of risks, coordination and policy-setting

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this chapter are R.1, 2, 33 and 34 and elements of R.15.[77]

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Belgium has a satisfactory understanding of ML/TF risks, although this varies from one authority to another, with the FIU (CTIF) having a better grasp of these risks. The supervisory authorities in the financial and non-financial sectors have sound knowledge of the ML/TF risks in their respective sectors, but the self-regulatory bodies (SRBs) lack a precise understanding of the ML/TF mechanisms that may affect their sectors, which limits their ability to prevent them. The investigating and prosecuting authorities generally have an empirical knowledge of the risks and types of ML, and a better grasp of TF risks.

b) The Belgian authorities are improving in their knowledge and understanding of the ML/TF risks and mechanisms associated with virtual assets, which still need further deepening in view of the high level of risk and the increased use of virtual assets by criminals in Belgium, both in ML and in TF.

c) Belgium has developed ML and TF National Risk Analyses (NRA), which were updated in 2023, producing reasonable results. However, the ML NRA does not take precisely and sufficiently into account the criminal patterns that are developing in unregulated fields. Corruption also appears to be on the rise as a significant ML threat but is not mentioned as such in the NRA. The TF NRA is based on field expertise but remains theoretical in certain respects and does not sufficiently contextualise the threats identified for Belgium.

d) In 2024, Belgium adopted an AML Action plan that defines four guidelines to steer its national policy and generally provides for the necessary specific measures. However, it does not reflect a strategic, long-term approach to stemming the sources of the main criminal activities in Belgium and tackling the links between ML and organised crime.

e) Belgium is implementing an operational strategy to counter TF, through which the authorities are focusing on all targets likely to be involved in TF activities.

[77] All these Recommendations are under review, see the Technical Compliance Annex (TC).

f) Belgium provides for exemptions from the AML/CFT regime (games of chance, certain activities of company service providers) which might no longer be justified by a low level of risk in the light of developments in the sectors concerned.

g) The Belgian authorities take account of the ML/TF risks identified in the country to a certain extent, but their activities are not systematically guided by or focused on the major ML risks.

h) Belgium has platforms providing appropriate channels for institutional coordination and cooperation: the Ministerial Coordination Committee to Counter the Laundering of Money of Illicit Origin (Comité ministériel de coordination de lutte contre le BC d'origine illicite) and the National Security Council (Conseil national de sécurité – CNS), which is responsible for TF issues. The AML Coordination Committee brings together most of the authorities responsible for defining national ML policies, but the CNS should ensure closer involvement with the CTIF and other authorities that play an important role in CFT.

i) Belgium has many formal and informal channels for operational cooperation, which lead to concerted action between competent authorities in areas linked to the main ML and TF risks.

Key Recommended Actions (KRAs)

Belgium should:

a) Increase the expertise of all competent authorities in the use of virtual assets for ML/TF purposes, based on existing experience, in order to improve the understanding of the risks associated with this sector, assess them at their relevant level for ML and for TF at national level, and define an appropriate strategic, legislative/regulatory and operational framework to improve the management of these risks.

b) Refine the mapping of alternative financial channels (e.g. cash, informal remittance systems) existing in the country and estimate their weightings so as to better highlight the ML/TF risks posed by these channels and take the necessary measures to manage them at national level.

c) Adopt an AML strategy based on the strategic priorities for Belgium, targeting major crime patterns (such as professional money launderers and the use of virtual assets), and link it with the existing strategies designed to counter predicate offences in the country, in order to stem the growing links between ML and organised crime.

Other Recommended Actions

Belgium should:

a) Develop a more systematic approach to horizontal ML/TF risks (such as the massive use of cash and the role of the port of Antwerp) in the ML and TF NRAs in order to improve the measurement of their impact on each of the affected sectors and promote a more appropriate response to the polycriminal activities identified.

b) Adopt a more granular approach to TF risks in the TF NRA and better measure the level of these threats in the Belgian context by using qualitative and quantitative elements to improve the understanding of their evolution in the country.

c) Include a dedicated TF component in the counter-terrorism strategy, based on the existing operational approach, and which can be adapted in response to changes in the country's TF risk profile.

d) Re-evaluate the application of the definition of games of chance in the AML Law to ensure that exemption from the AML/CFT framework is still justified on the grounds of low risk, in the light of the changes in lottery games over recent years.

e) Re-evaluate the scope of the AML Law with regard to company service providers' activities to ensure that the exemption on grounds of low risk is justified.

f) Ensure that the information in the ML NRA and the sectoral risk analyses developed by the competent authorities better inform each other so as to improve the alignment of the Belgian authorities' activities with the major ML risks identified in the country.

g) Extend the membership of the AML Ministerial Coordination Committee's Assembly of Partners to include SRBs and the Central Office for Seizures and Confiscations to enable all interested parties to contribute directly to the work.

h) Broaden the membership of the CNS Coordination Committee to include the CTIF, the customs authorities, SPF Finance-Treasury, the supervisory authorities for reporting entities and the tax authorities to enable all interested parties to contribute directly to TF activities.

i) Prioritise the project to reform the national AML/CFT coordination system initiated in 2023 and ensure that the CTIF's central role as an "operational" intelligence service in this new AML/CFT institutional architecture is maintained.

Overall Conclusions on IO.1

Belgium has a satisfactory understanding of ML/TF risks, which are regularly assessed by the competent authorities on a collaborative basis. One major weakness concerns knowledge and understanding of the ML/TF risks associated with virtual assets, despite the country's high exposure to these risks, as stated by Belgian authorities themselves, and the growth in ML and TF cases involving virtual assets. In addition, a significant proportion of criminal activity takes place outside the formal, regulated AML/CFT sector. These risks are therefore more difficult for the country to measure and understand, but there is no strategic approach to detecting them.

Actions are being taken to mitigate and control the risks identified, but these generally appear to be more commensurate with sector-specific risks than with risks identified at national level. An AML action plan was adopted in 2024, which is not aligned with strategic priorities for the country, suited to tackling the links between ML and organised crime. The operational strategy implemented to counter TF addresses all targets likely to be involved in TF activities.

Institutional and operational cooperation for AML purposes is generally effective, but it could be improved in the TF field by associating TF experts more closely with terrorism experts.

Major improvements are needed.

Belgium is rated as having a Moderate level of effectiveness for IO.1.

170. The evaluation team has based its conclusions on an examination of the documents submitted by Belgium and discussions with the Belgian authorities during the on-site visit.

Immediate Outcome 1

171. The structural, institutional and geographical characteristics of Belgium expose the country to significant financial and non-financial flows, which may be conducive to the development of criminal activities. The port of Antwerp is also a point of entry and an international logistics platform for legal and illegal goods and merchandise. Lastly, Belgium's high level of tax and social charges within the EU tends to encourage fraud (see the Introduction).

172. The 2023 ML national risk assessment states that Belgium is mainly exposed to criminal threats associated with cash trafficking, drug trafficking, social and tax fraud, other types of fraud and organised crime (see the Introduction). Belgium's ML environment is marked by a high degree of interconnection between criminal activities, which increases the opacity of the schemes and modus operandi leading to ML operations. Criminals tend to invest in sectors and activities not covered by the scope of the AML regime, which increases the complexity of ML networks and makes them less visible to the authorities. In addition, one of the main channels of ML in the country is the offsetting technique, which combines the massive use of cash with polycriminal activities such as social fraud, abuse of legal structures and drug trafficking (see the Introduction).

173. With regard to the terrorist financing (TF) threat, the 2023 national risk assessment concluded that the main threat relates to ex-foreign terrorist fighters and radicalised individuals ("lone wolves") via micro-financing involving new payment methods and small cash transactions, mainly of legal origin.

1.1. Country's identification, assessment and understanding of its ML/TF risks

1.1.1. General understanding of ML/TF risks

174. Belgium has a satisfactory understanding of the ML/TF risks to which it is exposed. The complex ML mechanisms based on closely interconnected criminal activities – drug trafficking, social and tax fraud, abuse of legal persons, trafficking linked to cross-border cash transportation and circulation – involving criminal organisations with international ramifications, with the port of Antwerp as a logistical hub, are clearly identified in the ML national risk assessment, which considers them to be major threats to the country. Links with TF, particularly through drug trafficking and organised crime, are also identified in the TF national risk analysis.

175. The understanding of the risks varies from one authority to another, with the FIU (*Cellule de Transmission des Informations Financières* – CTIF) having a better grasp of these issues. The supervisory authorities in the financial (National Bank of Belgium, (BNB), Financial Services and Markets Authority (FSMA)) and non-financial (SPF Economy) sectors have a sound knowledge of the ML/TF risks in their respective sectors, although they do not always connect them with the national risk context (see point 2.2.4). In general, the self-regulatory bodies (SRBs) are aware of the main risks affecting their sectors and of the most common types of risk that may affect them. However, they lack a precise understanding of ML/TF mechanisms, which limits their prevention capacity. The investigating and prosecuting authorities generally have an adequate empirical knowledge of the risks and types of ML, and a better grasp of TF risks (see below).

176. Generally speaking, the national risk assessments' conclusions do not always appear to be individually assimilated by the authorities and reflected in their approach to risks, which is still guided by a

primarily sectoral approach. National and sectoral risk analyses still insufficiently feed one another, which is detrimental to the development of a shared understanding of national risks by the competent authorities.

177. The national risk analyses carried out by Belgium (see below) and a number of recent cases reveal the growing use of virtual assets by criminals in ML and TF typologies. The Belgian authorities spontaneously cite these risks as one of the major growing threats to the country. Although some authorities have acquired and maintain a degree of expertise in this field (e.g. the FSMA and the Police, see IOs 3,8 and 9), the knowledge and understanding of the practical techniques and channels used for ML and TF purposes appear still generally limited. In addition, insufficient resources prevent the adequate monitoring of technical developments, that would help identify and anticipate changes in ML/TF risk.

1.1.2. ML risks

178. With regard to ML, the understanding of risks is based on the holistic approach adopted for the National Risk Analysis (ML NRA) conducted in 2019 and updated in 2023, in addition to numerous sectoral analyses (the most recent of which include sectors supervised by the BNB and by the FSMA; real estate sector, lawyers, company service providers/business centres). The methodology used to conduct the ML NRA and the stakeholders involved ensure a coordinated and coherent assessment of the country's risks. They produce reasonable results for the identification of priorities (see the Introduction), with one reservation linked to the fact that the updates are not always based on completely up-to-date data.

179. The ML NRA is largely based on information collected by CTIF from reporting entities and players in the formal sectors. This information provides a solid basis for the ML NRA, but may lead to a bias in favour of ML mechanisms that have already been identified, and may not sufficiently highlight emerging risks or risks that are less visible through CTIF channels. ML risks in Belgium originate largely from alternative financial networks, which are developing outside the regulated AML scope and reporting entities. It is therefore difficult to measure these threats, even if their existence and scale have been confirmed, notably by the police activities that bring these activities to light. Belgium lacks a systematic and structured approach to the detection of alternative financial circuits, especially those based on cash and illicit money transfer activities, which would be key to providing a more accurate picture of the scale of these threats and detecting new risk patterns.

180. Belgium is strongly affected by a number of cross-cutting risks, such as the massive use of cash and the role of the port of Antwerp, which impact the types and levels of risks affecting the country. These aspects are included in the ML (and TF) NRA without conducting a systematic, in-depth analysis of their influence, which does not fully characterise their importance in the Belgian context, or explain the organised and polycriminal nature of the networks that exploit these aspects. Corruption has not been identified as a significant threat, despite the existence of proven cases that have led to money laundering.[78]

1.1.3. TF risks

181. There is a sound understanding of the risks relating to TF. This is based primarily on extensive sharing of information and sources concerning TF techniques between the operational authorities responsible for terrorism and TF. This approach draws on direct feedback from field work and is adapted to the current situation, which is characterised by a moderate or even low level of TF risks, and by the nature of these risks, which are based mainly on simple micro-financing mechanisms. However, it does not enable the anticipation of changes in risks or the identification of emerging new threats and vulnerabilities.

[78] In particular, see OECD (2025), *OECD Anti-Bribery Convention - Phase 4 Evaluation Report of Belgium:Implementing the Convention and Related Legal Instruments*, Implementation of the OECD Anti-Bribery Convention, OECD Publishing, Paris

182. The current understanding of risk goes beyond what is reflected in the 2023 National Risk Assessment (TF NRA). The TF NRA paints an overall picture of micro- and macro-financing TF trends, which is useful for identifying changes in the threats identified (see the Introduction). However, the TF NRA is purportedly "academic" and does not always reflect the reality of the threats identified by Belgium. There is insufficient quantitative and qualitative data to provide a more granular analysis that would provide a realistic overview of the level of the different threats in Belgium and contextualise them for the country with a view to fostering a more dynamic understanding of TF risks and improving the identification of the high-priority areas of risk.

1.2. National policies and activities to address identified ML/TF risks

1.2.1. Policies and activities to address ML risks

183. The ML NRA led to the extension of the list of entities subject to the national AML/CFT scheme to include certain activities and professions associated with high ML risks: the professional football sector, safe deposit box rental, intermediaries in the purchase and sale of company shares, and security firms.

184. The ML NRA also led to the adoption, in March 2024, of an AML Action plan by the Ministerial Committee for Coordinating Measures Against Laundering Money from Illegal Sources, which is the national coordination platform (see the Introduction and section 1.5 below). This action plan ("AML Strategy") defines four guidelines for national AML/CFT policy: strengthen and monitor compliance with preventive measures; increase the transparency of legal structures and arrangements; reinforce detection and prosecution; optimise coordination and international cooperation. It sets out concrete recommendations to be implemented by the competent authorities in each of the four areas.

185. On the whole, these recommendations constitute appropriate measures for an improved AML/CFT policy in the country. For example, the proposed tightening of the AML/CFT supervision of diamond traders is necessary given the level of risk to which the country is exposed in this field and the limited number of controls currently in place (see IO.4). Similarly, the proposed intensification of measures against the misuse of legal persons seems essential (see IO.5), as does the introduction of measures to include virtual asset portfolios in the BNB's central register containing information on Belgian and foreign financial accounts and contracts ("PCC"). However, the measures included in the action plan are extremely ad hoc and do not reflect a strategic, long-term approach to the areas envisaged. This is notably the case for virtual assets, despite the recognition of the scale and extent of the associated risks in terms of both ML and TF (see the Introduction above). In addition, the envisaged measures are not based on an implementation timetable or on the prioritisation of actions.

186. Furthermore, the AML action plan lacks a vision based on strategic priorities for the country, which could be used to formulate in-depth responses to the major crime patterns that continue to develop in Belgium, highlighting the growing links between ML and organised crime. This approach should focus primarily on underground cash circulation and alternative financial networks, and be linked to the strategies already in place to combat the country's major underlying criminal activities – social and tax fraud, drug trafficking, organised crime and trafficking affecting the port of Antwerp. In particular, Belgium developed an action plan to counter social fraud in 2022, created a drugs commission in 2023 with a strong focus on trafficking at the port of Antwerp, and presented the fight against organised crime as one of the priorities of the government which took office in January 2025. All these policies include aspects that are also relevant to AML but which are not currently reflected in the AML action plan so as to foster the convergence and coherence of the policies pursued. In addition, the strategic approach will also need to learn from and build on the techniques implemented as part of the Sky ECC cases (see IO.7).

1.2.2. Policies and activities to address TF Risks

187. The Belgian authorities have demonstrated the existence of an operational CFT strategy, which was mainly developed following the 2016 attacks (see IO.9). This operational approach is based on close multi-disciplinary integration between counter-terrorism and TF measures, regular sharing of information on individual targets, and proposals for taking action against targets in the light of developments, notably via the Local Task Force (*Task Force Locales* – TFL) scheme, the Joint Data Bank (*Banque de données communes* – BDC) and the Joint Intelligence Centre/Joint Decision Centre (JIC/JDC) (see IO.9). This policy is based on the authorities' current capacity to take action against all targets likely to be involved in TF.

188. This operational approach has not been formalised and integrated into a dedicated TF strategy, including prevention and awareness-raising aspects among reporting entities, to complement the TER (Terrorism, Extremism and Radicalism) Counter-Terrorism Strategy (see section 15 below) for the TF component.

1.3. Exemptions, enhanced and simplified ML/TF measures

1.3.1. Exemptions

189. The 2017 AML Law (see the Introduction) provides for the possibility of exempting certain sectors from the application of the AML/CFT regime by Royal Decree (gambling establishments; operators carrying out financial activities other than money transfers, on a limited basis and ancillary to their main business), based on an appropriate risk assessment (see R.1, c.1.6 TC Annex). This possibility was implemented by the Royal Decree of 30 January 2019 exempting cafés offering games of chance from the obligations of the AML Law.

190. However, lottery games organised by the National Lottery do not fall within the scope of the 2017 AML Law, on the grounds that their characteristics pose a low ML/TF risk, as set out in the explanatory memorandum to the Law. However, the risks appear to have changed over the last few years, with the introduction of new games, including online games similar to casino games. The application of the definition of games of chance in the AML Law should therefore be reassessed.

191. For company service providers, the scope of the 2017 AML Law includes only one of the five categories of activities stipulated by the FATF – providers of head offices for enterprises (business centres) (see R.22 e. in the TC Annex). The main justification for not applying the AML Law to other activities is the fact that they are not subject to registration requirements, as they are not carried out on a professional basis on behalf of third parties in Belgium. The activity of incorporating legal entities is the only category for which reference to low ML/TF risk is made, as measured in the ML risk analysis conducted by Belgium in 2013. The current non-application of AML/CFT obligations to certain categories of company service provider (role of director or secretary of a legal person; role of trustee; role of nominee shareholder) is therefore not justified by a low ML/TF risk.[79] Furthermore, these activities seem to be evolving rapidly in the country, as are the associated risks, which should justify a rapid reassessment of the situation.

1.3.2. Simplified and enhanced measures

192. Belgium does not have a general system of simplified measures as such (see R.1, c.1.8 and 12, TC Annex).

[79] But rather by the fact that these professional activities are not carried out in Belgium, or at least only to a very limited extent, usually by professionals who are already obliged entities elsewhere.

193. Belgium has not defined an enhanced measures regime based on the conclusions of the ML NRA. However, since 2014, it has applied strict measures concerning the use of cash (maximum amount of EUR 3 000; ban for property sales), in response to the still massive circulation of cash in certain sectors, as illustrated by the ML NRA.

1.4. Objectives and activities of competent authorities and SRBs

194. The Belgian authorities take account of the ML/TF risks identified in the country to a certain extent, but their activities are not systematically guided by or focused on the major ML risks. The AML Action plan was adopted in March 2024 so it is difficult to assess its impact on changes in the authorities' activities. With regard to TF, the nature of the risks identified and the operational approach currently implemented by Belgium (see section 1.2 above) have led to greater consistency between the risks and the authorities' activities.

1.4.1. Alignment of AML objectives and activities

195. The CTIF relies on the conclusions of the ML and TF NRAs to identify the reports and cases to be addressed as a priority, and to carry out its strategic activities. Transmissions to the judicial authorities correspond largely to the major risks identified by Belgium, with a possible over-representation of suspicions linked to risks to which the attention of the reporting entities is especially drawn (see IO.6). The CTIF is also proactive in making proposals to adapt the AML framework and procedures to the modus operandi of criminals. For example, in response to the spread of the offsetting phenomenon, particularly to Brazilian networks, the CTIF and the Federal Prosecutor's Office started collaborating with SPF Finance in 2022 to develop a more effective response to the misuse of legal persons in support of polycriminal activities involving social fraud, drug trafficking, fraud, etc. The CTIF also launched a project with the Brussels Prosecutor's Office that led to a simplified procedure for the urgent freezing of transactions outside the framework of a criminal investigation with a view to enabling the Prosecutor's Office to seize and recover the maximum amount of funds (see IO.8). In 2023, these activities also prompted the CTIF to issue a report to the AML Ministerial Committee (see section 1.5 below) on improving the transparency of legal entities and preventing their abuse, notably by introducing measures to simplify and speed up the procedure for the judicial winding-up of shelf structures. The formalisation of these procedures is included in the AML action plan but has not yet been put into practice (see IO.5).

196. The CTIF's strategic analyses, which include operational elements, use the NRAs' conclusions to identify trends and typologies and to develop a more detailed understanding of them (see IO. 6). They reflect the main risks identified in the country, such as ML linked to illicit drug trafficking (2019, 2023), ML linked to Brazilian networks (2022) and the use of professional money launderers (2024).

197. The investigating and prosecuting authorities take action in reaction to criminal activities and do not adopt a proactive approach to aligning their activities with the main ML risks. The Police do not apply a detection strategy that specifically targets the predicate offences most frequently associated with ML, or ML itself (see IO.7). However, strong foundations have been laid to improve adaptation to the challenges posed by financial crime: the National Security Plan 2022/2025[80] explicitly recognises ML as a key cross-cutting pattern in organised crime and calls for the greater mobilisation of police forces. In response, the police have consolidated their capacity to tackle financial and economic crime, based on the use of specialist investigators. However, they are constrained by limited resources and apply the principle of the "TRIM" criteria restrictively when setting priorities (see IO.7). Therefore, further progress needs to be made in implementing a national security policy that takes full account of the challenges posed by financial crime.

[80] The National Security Plan | Federal Police

198. Regarding the customs authorities, the absence of a strategic approach to the supervision of cross-border cash movements and the reduced amounts detected or confiscated (see IO.8) reflect a lack of prioritisation of this field by the Belgian authorities, which is at odds with the significant ML/TF risk posed by international cash trafficking, identified in the 2023 NRA and in the previous NRA.

199. The activities of the financial sector supervisory authorities (BNB and FSMA) generally take account of the ML/TF risks identified in the country. The level of (residual) risk in the financial sectors is assigned on the basis of certain key risk factors in the ML and TF NRAs. High-risk financial activities are therefore the priority for AML/CFT supervision (see IO.3). The thematic activities undertaken by the BNB in recent years concern risk areas recognised as being important for ML/TF – de-risking, repatriation of funds and correspondent banking – even if they have not been identified as such in the NRAs. In this respect, it is also important for the sectoral assessments to inform the NRAs in order to develop coherent approaches to the sectors examined. Finally, certain risks identified as major in the NRAs – notably e-IBANs – have given rise to thematic measures by the supervisory authorities. For example, the main e-IBAN player on the Belgian market has been subject to reinforced supervision and various on-site and off-site inspection activities have been carried out by the BNB. The BNB has also developed a systematic approach to supervising FIs whose business model is based on e-IBAN activity. It has also contributed to the work undertaken at European and FATF levels on this subject.

200. Concerning virtual asset services, the FSMA[81] has carried out AML/CFT awareness-raising activities and inspections as part of the transitional regime for entities that were already operating as service providers prior to the extension of the AML Law's provisions to certain virtual asset service providers, and also when examining applications for registration (see IO.3). No applications for registration have been approved and no VASPs are currently registered, recorded or licensed in Belgium.

201. SPF Economy takes proper account of the risks posed in the NRAs when identifying the risks posed by diamond dealers, estate agents and business centres. The same applies to the ITAA for chartered accountants. The other supervisory authorities and SRBs do not take effective account of the ML/TF risks identified in the country for their activities (see IO.4). In this respect, the ML and TF NRAs must be systematically disseminated and communicated to all supervisory authorities and reporting entities.

1.4.2. Alignment of CFT objectives and activities

202. The activities of the Belgian authorities involved in the operational handling of TF are aligned with the main TF risks identified in the country (see section 1.2). The individualised handling of the targets primarily focuses on terrorism aspects, and more incidentally on the TF component (see IO.9). In addition, Belgium's lack of prioritisation of the detection of TF microfinancing risks linked to alternative financial networks, such as *hawalas* (see section 1.1), is likely to affect the country's ability to ensure the effective management of all TF risks.

1.5. National coordination and cooperation to develop and implement policy

203. Belgium has established institutional cooperation and coordination platforms on AML and CFT: the Ministerial Committee for Coordinating Measures Against Laundering Money from Illegal Sources (*Comité ministériel de coordination de la lutte contre le blanchiment de capitaux d'origine illicite* - Ministerial ML Committee) in 2013, and the National Security Council (*Conseil national de sécurité* – CNS) in 2015 (see the Introduction and R. 2 in the TC Annex), respectively.

[81] Supervisory authority for VASPs until 30 December 2024, see IO.3.

1.5.1. Institutional AML coordination and cooperation

204. The Ministerial ML Committee, chaired by the Minister for Justice, is responsible for establishing the general AML policy. It is assisted by a technical body – the AML Coordination College (Collège de coordination de la LBC d'origine illicite) – consisting of public-sector experts within an Assembly of Partners, on the one hand, and a Judicial Platform, on the other. One of the AML Coordination College's tasks is to develop and update the ML NRA. Following the adoption of the ML NRA in September 2023, an AML action plan was endorsed by the Ministerial Committee in March 2024 and transcribed into national AML policy. This institutional architecture for the coordination and cooperation of the competent AML authorities fulfils its remit of bringing together the authorities directly involved in AML, whose expertise is required to define a national AML policy. However, it has not yet led to the adoption of a sufficiently ambitious AML strategy (see the Introduction).

205. Furthermore, the Assembly of Partners of the AML Coordination College does not appear to include representatives of the SRBs of non-financial activities, and especially of sectors identified as being subject to the highest ML risk. Although they are apparently invited to contribute on an ad hoc basis, notably for the ML NRA, they need to be directly involved to ensure the representation of all authorities in charge of the sectors subject to AML obligations. The same applies to a certain number of private sectors, with a view to raising their awareness of AML issues and priorities (see IO.4).

206. In addition, and given the risk context in Belgium, the Central Office for Seizures and Confiscations (Office central des saisies et confiscations) should also be included in the Assembly of Partners. This additional member would reinforce the main priorities that Belgium should develop to improve its national AML policy (see sections 1.1 and 1.2 and IO.8).

1.5.2. Institutional CFT coordination and cooperation

207. The National Security Council (CNS), chaired by the Prime Minister, is responsible for overall intelligence and security policy in the country, including the strategic coordination of measures to counter terrorism and the financing of terrorism. It is assisted by a political body, the Strategic Committee (Intelligence and Security), which prepares for the CNS' meetings and ensures the coordinated implementation of its decisions, and a technical body, the Coordination Committee (Intelligence and Security), which is responsible for coordination, collaboration and exchanges of information between the members.

208. The CNS has not defined a standalone national policy on TF. The reference framework is the 2021 Terrorism, Extremism and Radicalism Strategy (TER Strategy), which sets out national counter-terrorism policy. While the TER Strategy does not explicitly target TF, the operational approach adopted covers TF aspects (see 1.2 above) and is conducted within the framework of the Coordination Committee (Intelligence and Security).

209. The composition of the Coordination Committee (Intelligence and Security) and the Strategic Committee reflects the operational and individualised approach adopted in these bodies, and the emphasis placed on enforcement aspects. Despite their expertise in the TF field and their combined information resources, which can further enrich the knowledge of the risks and their trends at national level, the CTIF, customs authorities and SPF Finance (Treasury) in charge of implementing asset freezes of listed entities, the supervisory authorities and the tax authorities are not permanent members of the Coordination Committee and the Strategic Committee (see R.2 in the TC Annex). However, the CTIF has chaired the Coordination Committee's TF platform and carried out the work on the TF NRA.

210. In this respect, the CTIF's role in the Belgian AML/CFT architecture should be reconsidered. It drives the development of the ML and TF NRAs, co-chairs and coordinates the work of the ML Coordination College and chairs the TF Coordination Committee's TF Platform. It is therefore identified as the main pillar

of AML/CFT activities by both the competent authorities and reporting entities. It also ensures de facto coordination between the ML Coordination College and the Coordination Committee (TF). In 2023 Belgium embarked on a project to reorganise national AML/CFT coordination, as set out in the AML action plan, with the aim of entrusting AML/CFT coordination to a single authority with no operational mandate. This approach should be continued and put into practice as soon as possible to optimise institutional cooperation and coordination with a view to providing a national response to the ML/TF risks identified, and to enable the CTIF to focus on its operational activities which are critical to the effectiveness of AML/CFT measures in Belgium.

1.6. National coordination and cooperation for operational purposes

211. Belgium has many formal and informal channels for operational cooperation between competent authorities, which promote concerted action between competent authorities in areas linked to the main ML and TF risks.

1.6.1. Operational coordination and cooperation for AML purposes

212. As far as the supervisory authorities are concerned, the CTIF and the BNB, on the one hand, and the FSMA on the other, interact on a regular basis to examine risk-related developments and to discuss the reporting policy for obliged entities and the quality of the reports received (on the basis of MoUs defining the interaction procedures). Tripartite meetings between the CTIF/BNB/FSMA also help to improve the understanding of the risks and emerging trends affecting the financial sectors. The CTIF and the FSMA have also cooperated with the Polish FIU in connection with a licence application from a Polish company wishing to operate virtual asset distributors (BTMs) in Belgium (see IO.3). The BNB and the FSMA also cooperate, especially on the supervision of FIs that simultaneously fall within their remit (i.e. institutions with multiple statuses such as credit institutions that are also registered as insurance intermediaries subject to the AML Law (brokers and non-exclusive agents operating in life insurance), or lenders that are subsidiaries of credit institutions or insurance undertakings). SPF Economy, which oversees several non-financial sectors, also maintains a productive dialogue with CTIF, mainly on risks and raising awareness among reporting entities.

213. Regarding investigations and prosecutions, the "Ecofin" network of experts in the fight against economic, financial and tax crime and corruption has been in place since 2015, bringing together the judicial authorities, the police and the CTIF, and supporting the public prosecutor's office in the conduct of criminal policy. It gives rise to useful exchanges of expertise, particularly on the modus operandi of criminals. The joint multi-disciplinary investigation teams (MOTEMs), established for tax matters in 2023 and based on the model of the existing MOTEMs for social matters, are another example of cooperation. These teams enable tax officials to collaborate directly on tax fraud investigations, reinforcing the expertise available for investigations. The number of tax MOTEMs remains limited at this stage and should enable the adoption of a more integrated approach to the fight against fraud. These initiatives generally improve the consideration of ML aspects, even though the surveys still effectively prioritise tax aspects (see IO.7).

214. More generally, the Belgian authorities frequently host liaison officers from other agencies involved in AML in order to facilitate operational cooperation and notably to obtain direct, real-time access to restricted information. For example, liaison officers from the Federal Police and Customs are appointed for the CTIF, and can access databases or other information (reports), which are useful for rapidly obtaining additional data on persons or companies mentioned in suspicious transactions and for enriching the reports received from reporting entities. The CTIF also uses liaison officers to gain access to sensitive information from civil and military intelligence services. The Central Office for Seizures and Confiscations also hosts police liaison officers to assist with asset-tracing investigations, magistrates to facilitate

collaboration with the public prosecutor's office and liaison officers from the SPF Finance to improve collaboration with the revenue collectors responsible for collecting criminal fines and enforcing court rulings.

1.6.2. Operational coordination and cooperation for CFT purposes

215. The handling of TF is based on an operational strategy revolving around multi-disciplinary consultation and decision-making platforms (see section1.2 above and IO.9). These platforms involve the police, including the central counter-terrorism service, intelligence services (civil and military) and the Threat Analysis Coordination Body (*Organe de coordination pour l'analyse de la menace* – OCAM). The judicial phase also gives rise to operational cooperation within MONITOR meetings at which information and investigations into terrorism handled by the Federal Public Prosecutor's Office are shared (see IO.9). They are attended by the judicial authorities – the judges in the anti-terrorism section at the Federal Prosecutor's Office – along with the intelligence services, OCAM, the police and the CTIF.

2 International co-operation

The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this chapter are R.36-40 and elements of R.9, 15, 24, 25 and 32.[82]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) Belgium has a comprehensive and adequate legislative, conventional and administrative framework for providing and requesting mutual legal assistance and extradition, as well as for asset recovery. Incoming and outgoing requests from countries outside the EU are centralised at SPF Justice. Requests to EU countries are submitted directly by the competent judicial authorities, in application of European provisions.

b) Belgium has shared available data, as well as case studies and examples of cases – mainly related to ML – that reflect its international cooperation activities. However, it has not comprehensively mapped the types of cases for which it has received requests or contacted its foreign counterparts, the category(ies) of predicate offence(s) and the result(s) obtained. This makes it difficult to assess the alignment of Belgium's international cooperation activities with the country's ML/TF risk profile, and the impact of requests on the country's international cooperation. In addition, comprehensive information on requests relating to the temporary or permanent immobilisation of goods or assets located abroad is not available.

c) The vast majority of incoming requests come from European countries, and mainly concern ML. The quality of mutual assistance provided by Belgium was deemed to be generally positive and constructive by the FATF Global Network jurisdictions that provided feedback on their experience. Belgium's average response times seem reasonable and SPF Justice has set up a system of reminders for incoming mutual assistance requests to ensure that responses to foreign counterparts are given within a satisfactory time frame.

d) Generally speaking, the number of outgoing requests to European countries is fairly low given Belgium's context and risk profile (see IO.1). However, the number of requests sent to non-European countries is much higher than the number of requests received, which shows that despite the difficulties, Belgium is seeking international assistance to resolve ML cases.

e) Through some case examples, Belgium has demonstrated that it is capable of dealing with complex ML cases involving international networks, notably by drawing on international cooperation initiatives, both within and outside the EU. However, in the absence of comprehensive data for all public prosecutors' offices in ML cases, it is unclear whether

[82] R.15, 24, 25, 32, 38 and 40 are under review, see the Technical Compliance (TC) Annex.

international cooperation measures are being implemented systematically, particularly for cases managed by district public prosecutors' offices outside Brussels. In connection with the observations made concerning the prosecution of ML (see IO.7), the lack of available resources hinders the Belgian judicial authorities in the systematic pursuit of these international ramifications.

f) The Belgian authorities are taking initiatives to remove obstacles to the prosecution of proceedings and to stimulate cooperation with non-EU countries, to which Belgium sends the most requests. Some of these initiatives have produced tangible results, notably extraditions with the United Arab Emirates and confiscations with Morocco. Many of these initiatives are ongoing or have not yet fully borne fruit. In a number of cases, public prosecutors have preferred to report offences to foreign authorities to enable them to take legal action at national level, particularly with regard to confiscations.

g) The Belgian authorities make extensive use of informal cooperation to combat ML/TF, whose quality has been praised by the Global Network members who have provided feedback. The CTIF, police and supervisory authorities in particular maintain regular and frequent relations with their foreign counterparts, mainly in the EU. These contacts are based on the sharing and exchanges of information, and can provide key operational support in matters requiring rapid action, such as TF.

h) The CTIF only requests information from foreign FIUs for judicial cases of ML where it possesses data on the natural or legal persons who are the subject of the request for information (see IO.7).

Key Recommended Actions (KRAs)

Belgium should:

a) Accelerate activities designed to facilitate international cooperation with countries outside the EU by involving, together with the SPF Justice, as necessary, the judicial and diplomatic authorities, in order to enhance the interactions with countries with which Belgium shares the most links, and in areas of major crime for Belgium.

b) Collect the necessary statistical data on mutual legal assistance and other forms of formal cooperation, in order to better measure its effectiveness, promote activation of international cooperation, promote the results obtained in major cases and identify the best practices.

c) Increase the judicial authorities’ resources to enable them to pursue systematically the international ramifications identified in ML cases, including through support from SPF Justice.

Other Recommended Actions

Belgium should:

a) Improve the monitoring of mutual assistance files (encoding of files, statistical data, type of mutual assistance requested, predicate offences, prioritisation, automatic reminders, etc.) with a view to improving the assessment of strengths and weaknesses of the system and implementing the measures required to ensure progress.

b) Encourage all the competent authorities to make systematic use of the informal cooperation channels available, particularly in ML/TF cases relating to areas of major risk for Belgium.

c) Facilitate international cooperation in criminal matters by allocating more human resources to the international cooperation unit at the Federal Public Prosecutor's Office.

Overall Conclusions on IO.2

International cooperation is a central aspect of AML/CFT activities in Belgium, given the country's characteristics, notably its size, its open economy and its geographical position at the heart of the EU. A highly significant proportion of the country's ML/TF circuits have international elements. In this context, the Belgian authorities make regular and fairly systematic use of informal cooperation to support their AML/CFT activities and provide high-quality support according to feedback from FATF Global Network members.

As far as formal cooperation is concerned, Belgium has demonstrated on several occasions that international cooperation has helped to solve complex ML cases, including the dismantling of networks with ramifications abroad in offsetting schemes. Nevertheless, in the absence of comprehensive data for all public prosecutors' offices in ML cases, it is unclear whether international cooperation measures are being implemented systematically, particularly for cases managed by district public prosecutors' offices outside Brussels. In addition, the general lack of resources for ML investigations and prosecutions (see IO.7), which was previously identified as an issue to be monitored in the 2015 MER, affects Belgium's ability to implement the resources required to systematically pursue the international component of ML cases.

Belgium has engaged in numerous collaborations with foreign partners, through diplomatic channels and bilaterally between judicial authorities, in order to facilitate and accelerate international cooperation. Some of these initiatives have already produced results and should be accelerated to maximise their full impact and ensure their long-term implementation.

In general, however, as Belgium has not comprehensively mapped the type of cases for which it has received requests or contacted its foreign counterparts, the category(ies) of predicate offence(s) and the result(s) obtained, it is difficult to assess the alignment of its international cooperation activities with the country's ML/TF risk profile and the impact of requests on its international cooperation. This especially applies to mutual assistance for asset recovery, a high-priority field of international cooperation for the country.

Major improvements will be required.

Belgium is rated as having fora Moderate level of effectiveness for IO.2.

Immediate Outcome 2

216. To assess Belgium's effectiveness, the evaluation team drew on interviews with the Belgian authorities, documents, information and case studies provided by Belgium,[83] and feedback from other countries in the FATF Global Network.[84]

[83] The statistical data provided is not always usable, notably because it does not always distinguish between data relating to ML and TF or to predicate offences. In addition, only CTIF is required to maintain statistical information on international cooperation with other FIUs (see R.33 in the TC Annex).

[84] Global Network countries that have provided feedback, including those approached on a bilateral basis under the new 5th round approach (para. 63 and 64 FATF Procedures): Albania, Germany, Spain, United States, France, Kazakhstan, Italy, Luxembourg, Northern Macedonia, Malaysia, Malta, Mexico, Netherlands, Poland, Thailand, Ukraine.

217. International cooperation is of major importance for AML/CFT activities in Belgium. Belgium's size and geographical location make it a trade crossroads and a transit country for people, goods, and services. It attracts significant financial and non-financial flows, which may foster the development of criminal activities, with multiple scenarios for the stages occurring in Belgium (destination, transit or origin of funds and associated crimes) (See the Introduction). Belgium's neighbouring countries are its main trading partners, and those with which interactions are most significant. In addition, the financial sector is characterised by the presence of multinational financial groups and numerous financial service providers operate in Belgium under the European passport, a factor that influences the intensity of exchanges with other authorities in EU countries.

2.1. Providing constructive, timely and quality mutual legal assistance and extradition

2.1.1. Providing evidence and locating criminals

218. Belgium has a central authority for international cooperation on mutual legal assistance and extradition – *Service Public Fédéral* (SPF) Justice (see the Introduction). A fourteen-staff unit manages cooperation requests from non-EU countries and is responsible for their management, quality, follow-up and confidentiality. They forward requests to the competent judicial authorities for their execution. SPF Justice collaborates closely with the Belgian public prosecutors' offices, each of which has a section specialising in international cooperation, as well as a magistrate in charge of this field ("*magistrat référent*"). The Federal Public Prosecutor's Office, as the first operational point of contact, and the Prosecutor General's Office in Ghent, which oversees the general policy of the Public Prosecutor's Office in this area, play a key role in this organisation.

219. For EU countries, and as in other Member States, requests for mutual legal assistance and extradition are communicated directly between national judicial authorities, which are responsible for their direct management, without the involvement of SPF Justice. This system of judicial cooperation is based on the principle of mutual recognition of court rulings in European countries. Belgian public prosecutors prioritise requests according to their content and the level of urgency indicated in the request itself by the requesting country.[85] In the event of any ambiguity or doubt about the degree of urgency, the judicial authorities contact their foreign counterparts to assess the urgency and attention to be given to the requests. Each prosecutor's office manages the requests received, using its own tracking system. In the majority of cases, the requesting authority follows up on the request.

220. In addition, the Federal Public Prosecutor's Office has priority jurisdiction for terrorism-related cases, which also includes TF (see IO. 9), including cooperation with EU and non-EU countries. To establish any links with existing investigations, all requests to and from other countries are managed directly by the Anti-Terrorism Section at the Federal Public Prosecutor's Office. The Federal Public Prosecutor's Office is therefore the point of contact for foreign judicial authorities and institutions such as Eurojust, Europol and Interpol in terrorism and TF matters.

[85] Section B of the EIO form or the equivalent section of an LR form

Table 2.1. Mutual assistance requests received

		2019	2020	2021	2022	2023	2024	Total
EU								
	EIO[86] - ML	71	87	154	176	185	147	820
	MLA requests[87] - ML	15	28	31	40	54	18	186
	EIO - TF	3	1	9	9	6	4	32
	Total	89	116	194	225	245	169	1 038
Non-EU (via SPF Justice)	ILR[88] - ML	18	12	37	20	50	64	201
	ILR – FT	0	2	3	2	2	2	11
	Total	18	14	40	22	52	66	212

Source: SPF Justice

221. Growing demand for mutual assistance has been observed since 2019. Between 2019 and 2024, Belgium received 1,215 requests for mutual assistance, 83% from European countries and 17% from non-EU countries.[89] This significant growth in 2021 and subsequent years can doubtless be explained by the resumption of international cooperation activities following the health crisis. It should also be considered in the context of ML projects with a strong European dimension, notably the Sky ECC project (see IO.7), for which Belgium has been approached by its European partners. The small number of TF-related requests is explained by the type of TF Belgium is currently facing, which is carried out mainly through microfinancing at domestic level (see IO.1 and 9). The biggest European partners in the TF field are France, the Netherlands and Germany.

222. The sizeable proportion of ML requests from EU countries reflects the intensity of interactions with these countries, especially Germany, France, Luxembourg and the Netherlands. Belgium has no specific information about response times but indicates that the deadlines imposed by European legislation are met (40 days for recognition, 90 days for enforcement).[90]

223. The non-EU countries with the highest number of requests are Switzerland (41), the United States (23) and Albania (21). The vast majority of the cases handled concern ML offences (the list of the main requesting countries suggests that some of the requests are linked to cases concerning tax fraud and organised crime), and only eight requests concern TF cases – from Libya, Thailand, Liechtenstein, Russia, the United States, Malaysia, Ireland and Switzerland. The median response time to the requesting judicial authorities is 170 days, which seems a satisfactory period and an improvement on the 2015 MER. This time frame includes the collection of the necessary information, legal analysis and transmission to the requesting authorities. SPF Justice has set up a reminder system for the judicial authorities to ensure that responses are provided within a satisfactory time frame.

224. No data has been provided on the ML cases linked to the requests, which makes it difficult to assess the effectiveness of Belgium's responses. However, the countries in the FATF Global Network that gave feedback on the information or answers provided by Belgium in the framework of requests for mutual assistance reported a very high satisfaction rate. The quality and relevance of the information provided, in addition to the response times, were deemed satisfactory, especially with regard to TF.

225. Belgium has not reported any refusal to provide mutual legal assistance to a foreign authority in ML or TF matters on grounds of the possible application of the dual criminality or *ne bis in idem* principle.

[89] The EIO and MLA requests figures relate to ML only. No data has been provided on mutual assistance requests received in relation to TF.

[90] Directive 2014/41/EU

Box 2.1. Example of cooperation in international mutual assistance

Agencies involved: SPF Justice, Belgian Public Prosecutor's Office, US judicial authorities

Facts: on 11 April 2024, Belgium received a request from the United States by secure e-mail for mutual legal assistance in connection with an investigation into suspected fraud and money laundering. The US authorities requested company incorporation documents, information concerning company officers and employees, and details of the commercial activities of company X. SPF Justice, in its capacity as the central authority, forwarded the request to the competent public prosecutor's office. A case reference number was created on 23 April 2024. On 25 July 2024, all the case documents were sent to the US authorities.

IO.2 relevance: thanks to Belgium's cooperation, the assistance requested by the US counterparts was provided promptly, despite the language barrier. This case demonstrates Belgium's commitment to tackling ML/TF proactively and in close collaboration with its international partners.

Outcomes: the US authorities received the case documents. They issued no further requests following receipt of the documents, which closed the file in Belgium. The absence of additional requests was a positive indicator of the requesting authority's satisfaction.

2.1.2. Extradition

226. Since 2019, Belgium has received 58 European arrest warrants for ML.[91] No data has been provided on the ML cases with which the requests were associated, which makes it difficult to assess the effectiveness of the responses. However, the feedback from FATF Global Network member countries on the assistance received from Belgium with their requests for extradition indicates an overall positive satisfaction rate.

227. Belgium lacks specific information on response times but states that European warrants are enforced within the time limits set by European regulations (60 days from the arrest; 10 days if the person consents to his or her surrender). Belgium cites the example of a request from Italy for the surrender of a person for handling stolen goods, ML and membership of a criminal organisation, which was processed in three weeks in 2024.

228. Since 2019, Belgium has received 12 extradition requests in ML cases from India (2), the United States (2), Armenia (2), Georgia (1), Ukraine (1), the United Arab Emirates (UAE) (2), Iran (1) and Northern Macedonia (1). Five cases have been closed and seven are in progress. In one of the cases involving large-scale money laundering, corruption and fraud, Belgium reported that it coordinated the countries involved (UAE, Germany, Switzerland) in order to facilitate the enforcement of requests in compliance with each country's criminal justice priorities. The average time taken to close an extradition application from a non-European country is 85 days, which illustrates the speed of enforcement.

2.1.3. Identification, freezing, seizing and sharing of criminal assets

229. Belgium has reported 39 European freezing orders (EFOs) received between 2019 and 2024, and two European confiscation orders (ECOs) relating to ML. These low figures show that the assets and

[91] This figure should be interpreted with caution due to the current coding system for mutual legal assistance requests received from the EU, which automatically records the main qualification only.

proceeds of crime tend to be moved out of Belgium,[92] even though requests from abroad received by the OCSC through informal channels (see IO.8 and point 2.2.3 below) could enable certain goods and assets to be immobilised at a preliminary stage of the investigations. Belgium has no information about the time taken to enforce EFOs and ECOs, and also lacks information about predicate offences and the outcomes of requests.

230. Belgium has not provided detailed data on the number of international letters rogatory (ILR) corresponding to requests concerning assets of illicit origin located in Belgium.[93]

2.2. Seeking appropriate and timely mutual legal assistance and extradition

231. Belgium applies for international mutual legal assistance in ML cases or cases involving predicate offences using a similar system to that used for incoming requests, through SPF Justice for non-EU requests, directly to the judicial authorities in the EU for ML matters, and directly by the Federal Public Prosecutor's Office in TF matters (see 2.2.1.).

232. The Belgian authorities are aware of the importance of international cooperation due to the generally transnational nature of offences linked to financial crime in Belgium (see IO.1). However, this point needs to be qualified where TF is concerned, as the incidents often occur in Belgium, which reduces the need for systematic international cooperation.

2.2.1. Seeking evidence and locating criminals

Table 2.2. Mutual assistance requests sent

		2019	2020	2021	2022	2023	2024	Total
EU								
	EIO – ML	65	62	90	81	124	89	511
	MLA requests - ML	6	2	5	7	6	5	31
	EIO - TF	6	8	6	3	1	1	25
	Total	77	72	101	91	131	95	567
Non-EU (via SPF Justice)	ILR - ML	72	36	40	59	70	59	336
	ILR - FT	0	0	0	1	1	0	2
	Total non-EU	72	36	40	60	71	59	338

Source: SPF Justice

233. In general, the level of outgoing requests is fairly low, which does not seem to be linked to the transnational nature of ML cases put forward by Belgium, but should be seen in the light of the small number of complex cases with foreign ramifications giving rise to prosecutions (see IO.7).[94] The vast majority of requests are sent to European countries. Since 2019, demand for European Investigation Orders (EIOs) has grown, with significant increases in 2021 and 2023, probably due to an acceleration of cases

[92] However, the figures should be interpreted with caution, given the judicial authorities' difficulty in extracting statistics due to the absence of a central system for monitoring mutual legal assistance requests in the EU, and the current coding system, which automatically records the main qualification only.

[93] The data is included in the number of ILRs from non-EU countries and cannot be extracted.

[94] However, these figures should be interpreted with caution, given the judicial authorities' difficulty in extracting statistics due to the absence of a central system for monitoring requests in the EU and the current coding system, which automatically records the main qualification only.

linked to offsetting networks, based on better knowledge of these networks and their European connections, and to cases linked to the Sky ECC cases (see IO.1 and 7).

234. Furthermore, Belgium does not comprehensively map the type of ML cases for which it has requested assistance from its foreign counterparts, especially European ones; nor does it map the category(ies) of predicate offence(s) and the result(s) obtained. This makes it difficult to assess the alignment of Belgium's international cooperation activities with the country's ML risk profile, and the effectiveness of outgoing requests for mutual assistance. Nor does Belgium have sufficient data to assess exchanges of TF-related information with other European countries. Belgium's biggest partners in TF matters are France, the Netherlands and Germany.

235. Outside the EU, the countries to which Belgium has issued the most requests for mutual assistance are Switzerland (32), Morocco (31), the United States (19), the United Kingdom (15), Turkey (14), the UAE (13) and Albania (12). The list of these countries reflects the mapping of cases and issues linked to international cooperation cited by Belgium (see below). On average, a Belgian request for mutual legal assistance takes 294 days to be implemented (the median period is 145 days).

236. Certain examples cited by both the Federal Public Prosecutor's Office and the district public prosecutor's offices (see IO.8, box on the Clown case) demonstrate the Belgian authorities' ability to handle complex ML cases and/or trace ML networks, notably by participating in international cooperation initiatives, both within and outside the EU. International letters rogatory, requests for mutual assistance for investigative purposes, and requests for joint action in the field ("joint action days") have produced results in major cases involving ML in offsetting or tax fraud proceedings. However, in the absence of comprehensive data for all public prosecutors' offices in ML cases, it is unclear whether international cooperation measures are being implemented systematically, particularly for cases managed by district public prosecutors' offices outside Brussels.[95] In connection with the observations made on the prosecution of ML (see IO.7), a lack of available resources hinders the Belgian judicial authorities' systematic pursuit of these international ramifications.

237. Joint investigation teams (JITs) are regularly assigned to ML matters, mainly with neighbouring countries, which facilitates the consultation of statements/reports ("*procès-verbaux*") and the performance of searches and hearings. These joint teams have proved useful in strategically important ML cases for Belgium, linked to drug trafficking and tax fraud. JITs have also been created in the TF field, especially with France for obtaining and processing evidence in the investigations linked to the Paris and Brussels attacks of 2015 and 2016.

238. However, the Belgian authorities are hampered by the difficulties and slowness of formal judicial cooperation procedures, mainly with non-EU countries. They therefore often make discretionary decisions to prevent the interruption of proceedings due to unmet requests for mutual assistance or lengthy delays causing the limitation period to expire, which is particularly important when the confiscation of goods or products located abroad needs to be envisaged. In some cases, Belgian public prosecutors prefer to report the offences to the competent foreign authorities ("*dénonciations*"), accompanied by the transmission of the complete case file. This strategy, implemented notably with Morocco and Albania, is based on a pragmatic analysis of foreign legal systems and aims to ensure the effective in situ confiscation of criminal assets. This is a practical way to counter impunity, but also to strengthen bilateral cooperation by relying on national legal frameworks that are sometimes better adapted to certain offences or to the location of the assets to be seized.

239. The available data shows that Belgium submits far more requests to non-European countries than it receives (see Tables 2.1 and 2.2 above), which shows that despite the difficulties, the judicial authorities are attempting to use international cooperation as an aid to resolve cases. Belgium is also actively striving

[95] Analysis based on a sample of ML cases reported by Belgium.

to overcome these obstacles through various initiatives. SPF Justice has renegotiated or is in the process of renegotiating a number of bilateral agreements in the field of financial crime with key countries in order to extend the areas covered. This applies to Morocco, which is one of the countries to which Belgium submits the most requests for mutual assistance, particularly in relation to drug trafficking and asset confiscation (see below).

240. The Federal Public Prosecutor's Office also cooperates with SPF Justice to resolve structural problems that hinder or limit international cooperation. A special unit has been created at the Federal Prosecutor's Office to foster more agile and productive international cooperation. This unit consists of four people, two of whom work part-time, which seems insufficient. Nevertheless, one example of this joint undertaking has been the identification of four high-priority countries as (presumed) safe havens for drug traffickers and for the funds resulting from the offences: Albania, Turkey, the UAE and Morocco. Action has been taken with each of these countries to find solutions. For example, the Federal Prosecutor's Office has signed a memorandum of understanding with its Albanian counterpart and the prosecutor's office specialising in organised crime and corruption. Two visits took place in 2024 to gain a better understanding of the legal framework and practices likely to achieve the best confiscation results. This approach has not yet produced concrete results, but it should help to improve and speed up the processing of Belgian requests. Also see the approaches adopted with the UAE (extradition) and Morocco (confiscation) below.

241. In the same vein, and to facilitate faster and more effective cooperation with the United States, another key partner of Belgium, a specialised cooperation unit has been set up at the Federal Prosecutor's Office. The members of this unit (specialised lawyers, investigating judges ("*juges d'instruction*") and magistrates) have been trained by their US counterparts to help improve their understanding of their expectations and procedures, and of the specific formal requirements of the requests they receive.

242. A similar approach has been adopted in the field of terrorism/TF – notably with Iraq – to improve the gathering of evidence. The Federal Public Prosecutor's Office has been involved in the Military Intelligence Services (*Services de renseignement militaire* – SGRS) initiative to establish a dialogue with the authorities. The Federal Prosecutor's Office hosted an Iraqi delegation of judges, police officers and members of intelligence services in 2021 to explain the ongoing investigations into terrorism and TF and to sign concrete agreements on further cooperation. Following this visit, the Iraqi authorities spontaneously exchanged information on an ongoing TF investigation.

243. The Federal Public Prosecutor's Office, SPF Justice and SPF Foreign Affairs are also taking joint action, including by organising formal, high-level missions ("*missions protocolaires*") involving the Prosecutor General to pave the way for more effective operational cooperation and make progress on judicial matters. This approach has produced positive results, as with Brazil, for example, in the Clown case.[96]

244. The Belgian authorities also exchange information with their counterparts on a regular basis, outside formal procedures but within the European framework for mutual assistance in criminal matters.[97] These discussions help to clarify requests quickly, resolve ambiguities and speed up the overall process, resulting in faster and better-quality formal police and judicial cooperation. In this way, the Federal Public Prosecutor's Office maintains a close dialogue and spontaneously exchanges information with its French, Dutch and German counterparts on TF matters, and also organises regular bilateral contacts. These close contacts have proved particularly valuable in times of crisis, particularly during the terrorist attacks of 2015/2016. They have also been useful in connection with the "Syrian wallet" case, notably by providing the basis for launching investigations (see IO.9).

[96] Belgium has also drawn on the EMPACT project to provide resources for implementing and running judicial coordination.

[97] Convention of 29 May 2000, Art. 7

Box 2.2. Cristo case

Agencies involved: The CTIF, an investigating judge ("juge d'instruction") at the Brussels Court of First Instance (Tribunal de première instance – TPI), the Spanish FIU, and the investigating and prosecuting authorities of the countries concerned.

Facts: Based on information contained in suspicious transaction reports (STRs), the CTIF wished to conduct a more detailed analysis of the activities of a Spanish law firm, which appeared to operate as a collection, transfer and reinvestment centre for funds of dubious origin, including EUR 13 million from a group of companies based in Belgium whose actual activities were inconsistent with the financial flows they handled, and which appeared to be controlled by a criminal organisation actively engaged in money laundering. Thanks to the information received from CTIF, the case was referred to an investigating judge at the Brussels Court of First Instance, who sent seven requests for European mutual assistance and eight additional requests, all of which were answered. Three international letters rogatory were also sent to Morocco, the UK and the UAE. Simultaneous searches were conducted in Spain and Belgium.

IO.2 relevance: The mutual assistance requests required for the investigation were sent to all parties that were able to provide information, in accordance with the mutual assistance procedures in force within and outside the EU.

Results: International cooperation was essential in order to obtain information and justify the inconsistency in invoices noted by the CTIF. The analyses identified the network and its cross-border interconnections. Some of the law firm's Moroccan clients have been subject to tax reassessments in their own countries. The presence of a liaison judge in Morocco produced results, but required numerous follow-ups. The case is still under investigation.

2.2.2. Extradition

245. Belgium issued 80 European arrest warrants (EAWs) between 2019 and 2024. Requests for these EAWs are increasing and remain at a higher level than incoming applications, which confirms that offenders are fleeing the country. Belgium lacks sufficient data on the predicate offence category(ies) and on the results of its EAWs to assess the effectiveness of its actions and their alignment with the country's ML/TF risk exposure. However, the Belgian judicial authorities attest to the generally rapid implementation of these requests due to the application of a simplified procedure.

246. Belgium reported 25 extradition requests to non-EU countries between 2019 and 2024, ranging from 0 in 2020 (health crisis) to 8 in 2023, all concerning ML offences. Nine were granted and led to an effective surrender; 13 are currently being processed, accompanied in most cases by arrests and ongoing legal proceedings in the executing country; three were refused – one because priority was given to a European arrest warrant issued by France, where the person was extradited, and the two others because the wanted persons had left the territory of the executing country. On average, it takes 225 days for a request to be implemented (median 138 days), which seems satisfactory.

247. Eleven of these 25 requests were sent to the UAE. Belgium has taken steps to facilitate these procedures. Several missions have been carried out by Belgium and regular meetings have been held with the Emirati authorities to gain a better understanding of the local judicial system and overcome the difficulties associated with blocked extraditions, and with requests to identify and locate assets in asset investigations that may lead to confiscation. A judge specialising in international cooperation with the UAE

has been appointed to the Federal Prosecutor's Office. These measures have led to four extraditions for offences relating to financial crime since the extradition treaty was signed in 2021.

2.2.3. Identification, freezing, seizing, confiscation and sharing of criminal assets

248. The Belgian authorities lack detailed information about requests for mutual assistance relating specifically to the temporary or permanent immobilisation of goods or products located abroad, which makes it difficult to assess the effectiveness of international cooperation activities in this matter and their alignment with the country's risks. However, they stress that this area poses some of the greatest difficulties in judicial matters, which are often resolved by reporting the offences to the competent foreign authorities ("*dénonciations*", see above).

249. To make headway in this matter, Belgium has implemented measures, as with Morocco, which is one of the countries to which Belgium issues the most mutual assistance requests for the confiscation of assets, notably linked to drug trafficking (around 40 per year). A memorandum of understanding to strengthen cooperation and facilitate "*dénonciations*" was signed in October 2024: seven of the 14 transmitted in recent years have been processed, four have led to convictions in Morocco, three of them with confiscations; three have led to dismissal or acquittal and one is still being processed. The bilateral agreement on mutual legal assistance between Belgium and Morocco is being extended to cover asset confiscations. This should notably enable the authorities to go beyond the hitherto applicable freezing/seizure measures, and lead to the confiscation, in Belgium's favour – of property or real estate that could not previously be confiscated by the Belgian authorities. Belgium's only liaison judge posted abroad has also been appointed in Morocco.

250. The sharing of criminal assets and confiscated property with the countries concerned is carried out in accordance with European rules (shared equally when the amount of the confiscation exceeds EUR10,000) and in accordance with the applicable international conventions with non-EU countries (see IO.8).

2.3. Other forms of international cooperation for AML/CFT purposes, including asset recovery

251. The Belgian authorities make extensive use of other forms of cooperation, including informal cooperation, to counter ML/TF.

2.3.1. FIU

252. The CTIF shares information with foreign FIUs via secure platforms – FIU.net (for European FIUs) and Egmont Secure Web. The CTIF also exchanges information with FIUs that are not members of these networks, based on memoranda of understanding to ensure the security of communications.

Table 2.3. The CTIF's incoming and outgoing requests

Incoming international cooperation (requests or communications received by the CTIF)						
	2019	**2020**	**2021**	**2022**	**2023**	**2024**
Requests for information	381	475	601	624	682	611
- from the EU	320	427	531	564	624	561
Spontaneous reports	1081	522	911	474	491	494
- from the EU	173	304	549	436	442	435
- from North and South America	827	213	350	29	43	33
Outgoing international cooperation (requests or communications sent by the CTIF)						
	2019	**2020**	**2021**	**2022**	**2023**	**2024**
Requests for information	821	711	338	307	317	346
Spontaneous reports	282	280	379	635	759	1 134*

Note: *Including 1,180 reports issued in connection with correspondent banking transactions.
Source: CTIF

253. The CTIF employs three full-time staff to manage and filter incoming requests for information from foreign FIUs. The requests follow the same process as for STRs (see IO.6 - urgent, priority and normal requests). These three people process requests requiring no analysis and whose response only requires consultation of the CTIF database. Requests requiring more in-depth analysis are forwarded to specialist analysts in the Operational Analysis Department, who are responsible for replying to foreign counterparts.

254. As far as incoming requests are concerned, the vast majority (90%) of requests for specific information concern European counterparts, particularly from neighbouring countries. The origin of unsolicited information linked to Belgium is more varied. The high number of spontaneous reports from North and South America between 2019 and 2021 was mainly due to FinCEN reports relating to TF in the post-terrorist-attack period. In 2022 and 2023, the exchanges were linked to cases involving various types of fraud, tax fraud, virtual assets, TF and criminal organisations, and drugs.

255. The assistance given by the CTIF to foreign counterparts is identical in its scope and exhaustiveness to that provided to national authorities (see IO.6). For example, the CTIF provides information contained in its database or to which it has access, reports police or judicial investigations, and transmits financial information such as bank accounts, details of financial movements, or information on the beneficial owners of legal persons (with the deficiencies noted at national level in the quality of data on beneficial owners, see IO.5).

256. All requests for information received must be answered as quickly as possible and in any event within the deadlines set out in the FIU.net and Egmont Secure Web procedures. Weekly monitoring is carried out and reminders are sent to all analysts to ensure that these deadlines are met. The satisfactory quality of the information transmitted, including its accuracy and speed, has been confirmed, notably by feedback from the countries in the FATF Global Network.

257. The vast majority of the outgoing requests issued by the CTIF to its foreign counterparts concern European countries, both for specific requests for information and for spontaneous reports on information held by the CTIF. The overall drop in requests for information from 2021 onwards should be seen in light of the increase in spontaneous exchanges sent to foreign FIUs, as evidenced by the near doubling of these exchanges in 2023. This trend is driven by a number of changes in operational policy designed to improve efficiency, with the development of a new approach to tackling the ML cases linked to offsetting and TBML more effectively (see IO.6), as well as spontaneous reports concerning correspondent banking in response to an aspect prioritised at national level (see below). In addition, the entry into force of a new method of international exchange (XBD, "cross-border dissemination", which mainly concerns cases relating to fraud)

has had an impact on outgoing requests. Lastly, the drop in the number of TF-related cases (see IO.9) is reflected in these figures.

258. Since 2022, the number of spontaneous reports issued by the CTIF on correspondent banking has increased substantially following the COBA project launched with the professional association of financial institutions (FEBELFIN) in 2021, which was also addressed by a European project. The aim of this project was to improve the content of COBA reports sent to the CTIF by the four largest Belgian banks, in order to improve the characterisation of circumstances surrounding the suspicious transactions identified and to ensure that the information transmitted could be passed on to the law enforcement authorities. The analysis of COBA reports led to the transmission of 1,368 spontaneous reports to 54 different FIUs between January 2022 and July 2024. Feedback from several foreign FIUs indicated that the information provided by the CTIF was clear, comprehensive and qualitative, that it was an important source of new information, and that they wished to share the information with their competent national authorities. The international exchanges initiated by the CTIF in this area have therefore contributed to the fight against criminal activities carried out through correspondent banking, particularly in connection with corruption, TBML and organised crime networks.

259. Offsetting-related networks are another major field in which CTIF shares information intensively with its foreign counterparts, with a particular focus on Brazilian networks, characterised notably by their transnational dimension and their close links with Brazil and Portugal (see IO.7). The CTIF's requests concerning natural or legal persons involved in these networks have enhanced the analyses and enabled the reconstitution of the criminal chain and its international ramifications, producing significant results.

260. In the Sky ECC case (see IO.7), the CTIF played a key role in supporting operational activities, including by contacting foreign counterparts and prioritising the collection and processing of information gathered on the identified entities through the decryption of communications by the police. These actions led to the referral of 89 cases to local prosecutors' offices.

261. The CTIF has also increased the number of spontaneous reports in a number of TF-related cases, such as the "Syrian wallets" (see IO.9). The available identification data on the "collectors" (the central link in the system for transmitting money to Belgian FTFs) identified by CTIF was shared after an investigation with all the FIUs of the countries involved with a view to triggering further research and mapping the networks to which these people belonged. Through four spontaneous reports issued between 2017 and 2022, the identification data of 336 collectors was shared with international partners.

262. The goAML tool in place since the end of 2024 (see IO.6) should provide CTIF with quantitative granular information on the type of requests received and issued, as well as on the time frames, nature and quality of the responses received and issued. Through the examples of cases cited above and illustrated below, the CTIF nonetheless demonstrates that it seeks to cooperate with its foreign counterparts in sectors with a high ML/TF risk.

Box 2.3. Case of notarial reports

Subject: ML through real estate acquisitions in Belgium

Agencies involved: CTIF, United Arab Emirates (UAE) FIU, Mauritian FIU, German FIU, French FIU

Facts: In 2019, the CTIF received an STR from a notary in connection with the acquisition by a French couple (Mr and Mrs X) of a property in Belgium worth EUR 1,660,000. The property was acquired through international transfers totalling more than EUR 1,875,000 to the account of the notary's office. These funds came from several bank accounts held by Mr X in the UAE, Mauritius and Germany. Mr X was unable to justify certain funds from Hong Kong, China.

IO.2 relevance: The CTIF requested the cooperation of its counterparts in the UAE, Mauritius and Germany to obtain additional information on the origin of the funds and other relevant information.

Results: The information received from the contacted FIUs enabled the CTIF to demonstrate the use of complex structures (multiple bank accounts and shell companies) to launder funds of illicit origin in Togo's oil sector. The investigations are still in progress.

Box 2.4. Case involving the Ukrainian and Croatian FIUs

Subject: Receipt of almost EUR 2 million originating from Croatia into Belgian bank accounts with the funds suspected to be of fraudulent origin. One of the accounts was held by a Belgian diamond trading company.

Agencies involved: CTIF, Croatian FIU, Ukrainian FIU, one Belgian bank, the Belgian judicial authorities and the OCSC.

Facts: At the end of April 2024, the CTIF received a spontaneous report from the Croatian FIU concerning Mr X, a Ukrainian national, manager and BO of the company A, involved in the purchase and resale of three hotels in Croatia for a total value of EUR 38 million using funds of dubious origin linked to Ukraine. Mr X subsequently made various transfers into an account held by his daughter Y with a Belgian bank.

IO.2 relevance: The CTIF obtained additional information from the FIUs of Ukraine and Croatia, as well as from stakeholders (bank, central point of contact (PCC)), which was used to trace suspicious funds used in Belgium, notably to finance the share capital of a Belgian company C whose activities included trading in diamonds, other precious stones and jewellery.

This additional information enabled the CTIF to reveal that a proportion of the suspicious funds had been transferred to Y to finance the share capital of company C whose activities included trading in diamonds, other precious stones and jewellery. The financial analysis also showed that another account held by Y with the same bank had been credited on a monthly basis on behalf of an account held by company A in Croatia. Some of this money was used for payments to a diamond exchange in Antwerp.

Results: Due to the seriousness and urgency of the matter, the CTIF notified the bank concerned that it was blocking the execution of any debit transactions on all accounts opened in the names of Y and company C. The CTIF also forwarded the file to the Belgian judicial authorities as a matter of urgency and simultaneously informed the OCSC. It also passed on additional information received, particularly on developments in Ukraine, to the Public Prosecutor's Office. Sums totalling EUR 2,022,987.26 were seized and transferred to the OCSC. The case is still under investigation.

263. Since 2019, and in application of a European provision,[98] when the CTIF receives an STR concerning another EU country, it must automatically externalise the STR data to its foreign counterparts in a standardised manner. This gives rise to cooperation in the form of XBR ("Cross-border reporting") – receipt of a report issued by an obliged entity whose main activity is carried out under the freedom to provide services from Belgium and which is therefore subject to the Belgian AML/CFT Law, but whose reports predominantly do not concern or have no direct link with Belgium; and XBD ("Cross-border dissemination") – receipt of a "conventional" report that may be of interest to one or more other European FIUs.

Table 2.4. XBD/XBR dissemination for European FIUs

Number of	2019	2020	2021	2022	2023
XBR	38	893	8.021	11.154	19.574
XBD	47	114	613	323	193

Source: CTIF

264. The massive increase in XBRs from 2021 onwards has been due mainly to STRs relating to payment service providers who moved to Belgium after Brexit under the European passport mechanism. These reports correspond to transactions conducted via these payment service providers with entities located in the country of the recipient FIU. Outgoing XBD exchanges (launched in 2021) mainly concern fraud-related cases, for which the CTIF changed its internal processing policy at the same time, entailing less analysis with a view to referral to the courts (and therefore fewer requests abroad) but more XBDs.

265. With regard to TF, the CTIF may request information from its foreign counterparts on natural or legal persons for whom it does not already hold information. It frequently does so to meet the needs of legal proceedings. This option should also be used in relation to ML where the CTIF does not already hold data on the persons concerned, in order to speed up the international cooperation process on ML and support international investigations by the judicial authorities (see IO.6 and 7).

2.3.2. Law enforcement agencies (LEAs)

266. At the police level, the Federal Police's Directorate for International Police Cooperation (*Coopération Policière Internationale* – CGI) is responsible for managing and processing international cooperation at operational level. This department liaises between Belgian police units and their foreign counterparts. It is staffed by 20 people and operates 24/7. There is also a back office staffed by 60 people and 20 lawyers and translators. It also oversees of the network of police liaison officers.

267. Belgium has 15 liaison officers abroad (including in Romania, Spain, Albania, the United States, Brazil, Colombia, Morocco and Turkey), six at Europol and 60 foreign police liaison officers accredited by Belgium (including from the United States, Romania and France). Belgium can also ask Dutch liaison officers to request international cooperation from third countries, e.g. with the UAE. In TF matters, the central police service dedicated to terrorism and FT (DJSOC-Terro, see IO.9) also has a secure line of communication with the French domestic intelligence services (DGSI), which illustrates the links and the need for close cooperation between the two countries.

268. The CGI cooperates closely with its foreign counterparts, mainly through Interpol and Europol, on ML and TF. Information exchanges are based on secure channels. The requests mainly concern information relating to legal persons, such as company directors, or vehicles, especially with regard to their owners.

[98] Article 53.1 of the Fourth AML/CFT Directive transposed by Article 124 of the AML Law of 18 September 2017

However, when it comes to bank accounts, tax information or the location of assets, these issues require more complex and formalised judicial cooperation (see sections 2.1.1 and 2.1.2.).

269. The management of requests for police cooperation is governed by strict time frames, which are adapted according to the urgency of the matter. A “Flash” request is processed within an hour and an urgent request within 24 hours, while “normal” requests are processed within 10 days. The FATF Global Network member countries that provided feedback on cooperation with the Belgian police services have expressed their satisfaction.

270. The police authorities send and receive ML/TF-related requests via Europol and Interpol. The police authorities also reported a number of cases illustrating joint work with foreign police authorities. One of the most striking examples is Sky ECC. An operational task force was set up by Europol, in which 25 countries participated, with Belgium being one of the driving forces (see IO.7).

271. The Belgian police services (DJSOC-Terro and the Brussels Federal Police Criminal Investigation Department) also actively cooperated with Europol on the *Syrian wallets* cases (see box in IO. 9), participating in the dedicated Europol taskforce which drew up investigation plans with the countries concerned. The Belgian police also contributed to the use of information transmitted by police services in other EU countries via Europol. Lastly, cooperation between the Belgian authorities as a whole (Federal Prosecutor's Office, CTIF, Federal Police), Eurojust and Europol has enabled the identification of the financing channels used.

272. In the TF field, the Federal Public Prosecutor's Office participates in the activities of Eurojust, focusing primarily on terrorism but also including TF aspects. For example, Belgium contributes to the Counter Terrorism Register (CTR), in place since 2021, which centralises judicial information on investigations, prosecutions and convictions in EU countries and enables links to be established between ongoing proceedings.

Authority responsible for asset recovery

273. Belgium’s Central Office for Seizures and Confiscations (*Office central des saisies et confiscations*) is the national contact point for the EU's Asset Recovery Office Platform (ARO) and the international Camden Asset Recovery Inter-Agency Network (CARIN). These two networks facilitate informal contacts and rapid exchanges of information on asset tracing, both for suspects under investigation (with a view to asset freezes) and for convicted offenders (with a view to asset recovery). Overall, incoming and outgoing requests for information via the ARO and CARIN networks have been increasing since 2019 (see IO.8).

2.3.3. Supervisors of FIs, VASPs and DNFBPs

274. The BNB maintains frequent bilateral contacts with other AML/CFT supervisory authorities, both within and outside the EU. These contacts include exchanges of information on supervised financial institutions and the results of inspections, the coordination of respective supervisory monitoring activities, which may lead to the organisation of joint inspections, and the identification of ML/TF risks.

275. For example, in 2022, the BNB exchanged information with its French counterpart (ACPR) in connection with a report of an infringement involving the management of a French credit institution and its branch in Belgium. The two authorities organised an inspection in 2023 covering the identified concerns. In 2024, the BNB and its Irish counterpart, the Central Bank of Ireland, travelled to Lithuania on a joint visit to the operational teams at the shared service centre of a payment institution based in Ireland, which offers services in Belgium through a large network of agents, in order to assess the compliance of the AML/CFT process and identify ML/TF risks. This action enabled them to coordinate their supervisory activities. Also in 2024, the BNB, with the European Central Bank’s agreement, contacted the New York State Department

of Financial Services to investigate the veracity of the facts alleged in a report indicating offences concerning the Belgian subsidiary of a US credit institution.

276. The BNB also collaborates with the EU supervisory authorities for financial institutions operating in the territory of three or more EU Member States, including Belgium, which requires the creation of supervisory colleges (see IO.3). At the end of 2020, the BNB took part in the first colleges run by other supervisory authorities and organised the first meeting of an AML/CFT supervisory college for a Belgian credit institution. On 31 December 2024, the BNB had organised 33 college meetings for 17 financial institutions (credit institutions, life insurance companies, payment and electronic money institutions). It also took part in a total of 58 colleges organised by other European supervisory authorities, including 17 with France, nine with the Netherlands and eight with Luxembourg. In addition to closer cooperation, the colleges develop joint supervision strategies, particularly when significant ML/TF risks are associated with group entities. The BNB also cooperates with the European Central Bank within the framework of the Single Supervisory Mechanism to check the fit and proper requirements of the managers and shareholders of credit institutions qualified as significant (see IO.3).

277. The FSMA consults its foreign counterparts on a regular basis when conducting the fit and proper checks of the directors and shareholders of the financial institutions it oversees. It also receives requests to this effect from foreign authorities. In addition, FSMA participates in 19 AML/CFT supervisory colleges set up at European level for financial institutions operating in more than one EU Member State (see above).

278. In its capacity as the AML/CFT supervisory authority for VASPs (see IO. 3), the FSMA examined registration applications of Belgian VASPs. It systematically consulted the foreign authorities of the countries concerned when the manager(s) or shareholder(s) had declared that they had held positions with a company under the supervision of another foreign authority, or when the entity was a company that was already regulated in another country. The FSMA requested information from the Polish, Spanish, French, Dutch, German, US and Luxembourg authorities.

279. The competent authorities responsible for supervising DNFBPs – SPF Economy, Belgian Gaming Commission, Belgian Audit Oversight Board – cooperate and maintain contacts with their foreign counterparts, particularly from neighbouring countries. Examples of this cooperation include sharing experiences, exchanging information and cooperating on supervision issues. In most sectors, the intensity of exchanges with foreign counterparts is relatively limited because DNFBPs rarely engage in international activity. However, the diamond sector is internationally oriented in many respects (e.g. origin and destination of the products, partners in the production chain, origin of the customers, Antwerp-based sites of entities linked to foreign groups). SPF Economy's activities reflect this international scope, especially through its active participation in various mechanisms (G7 sanctions, Kimberley process, etc.) and technical contributions to them, which shed light on the sector's risk context.

2.3.4. Customs and tax authorities

280. As part of its remit, and therefore for all matters relating to customs offences, Belgian Customs receives requests for information from other customs administrations and also issues requests to them.[99] Information sharing between Belgium and non-EU countries is based on bilateral agreements signed by Belgium and non-EU countries on a reciprocal basis. Information is shared between Belgian Customs and EU countries via Europol using the SIENA communication channel. Information can also be shared via the Belgian liaison officer at Europol. Customs also share data on cash offences with Europol via the SIENA system to enable the cross-referencing of this data with the data in their database. For all AML aspects that

[99] Mutual assistance under Regulation 515/97 and the Naples II Convention

do not constitute customs offences, Customs information is exchanged through the CTIF and via mutual legal assistance with the authorities of third countries.

281. The tax authorities do not report any international AML/CFT cooperation activities directly, but the specific tax fraud-related ML information they report to the CTIF is used in international cooperation with other FIUs, or by police or judicial authorities in the context of intelligence exchanges on the basis of judicial treaties or international letters rogatory.

2.3.5. International cooperation on information about legal persons and legal arrangements

282. Basic information on legal entities and arrangements is freely available in four languages (French, Dutch, German and English) to any interested party, including foreign authorities, via the Banque-Carrefour des Entreprises register[100] (see IO.5). The information on beneficial owners that CTIF or the supervisory authorities of financial institutions, or other competent Belgian authorities may exchange with their foreign counterparts (see above) includes beneficial ownership information to which they may have access via the obliged financial institutions.

283. Foreign authorities may access information on beneficial owners held in the UBO register, either in a request sent to SPF Finance (Treasury), or via the European Beneficial Ownership Register Interconnection System (BORIS) for EU authorities connected to this system, to which the UBO register has been linked since April 2024.[101] For requests sent to the Treasury, a legitimate interest must be demonstrated in order to verify that the requesting authority is acting as a competent authority. The Belgian authorities may also obtain and transmit information on beneficial owners available at national level on behalf of their foreign counterparts in the EU (see R.24 and 25 in the TC Annex).[102] However, the shortcomings of the UBO register are currently hampering the Belgian authorities' efforts to provide verified and up-to-date information to their counterparts (see IO.5).

[100] Banque-Carrefour des Entreprises - Services for everyone | SPF Economie

[101] General information on finding beneficial owners | European e-Justice Portal

[102] At the end of the on-site visit (14 February 2025), the UBO register was not yet connected to the central European Beneficial Ownership Register Interconnection System (BORIS).

3 Financial sector and virtual asset supervision and preventive measures

The relevant Immediate Outcome considered and assessed in this chapter is IO.3.[103] The Recommendations relevant for the assessment of effectiveness under this chapter are R.9-21, 26, 27, 34 and 35 and elements of R.1, 29 and 40.[104]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) The main supervisory authorities of the financial sector - BNB and FSMA - have adapted their procedures to effectively supervise market access. The detection of illicit financial activities remains insufficient, particularly with regards to hawala-type transfers and transactions involving virtual assets, even though these channels are considered to be associated with a very high ML/TF risk.

b) The identification of ML/TF risks by the BNB and the FSMA has improved, thanks to the performance of generally satisfactory sectoral analyses (SRAs) - a second for the BNB in July 2023 and a first for the FSMA in September 2024, and a formalised dialogue with the CTIF. The understanding of risks by competent authorities is broadly satisfactory for credit institutions (CIs) and bureaux de change. The alignment between the National Risk Assessment (NRA) and the SRAs is not entirely satisfactory, and the divergences in assessment noted between the NRA and certain parts of the SRAs undermine financial institutions' (FIs) understanding of risks. Exchanges with FIs on risks are not sufficiently developed.

c) The understanding of risks by CIs is generally adequate, while it remains variable among other FIs. In particular, significant shortcomings remain among FIs offering certain innovative products, such as virtual IBANs, where BNB supervision revealed insufficient control of risk. FIs supervised by the FSMA have, in general, improved their understanding of their risks, although this remains variable. This understanding is based mainly on the SRAs, CTIF reports and internal findings, while the ML and TF NRAs remain little known.

[103] When assessing effectiveness under Immediate Outcomes 3, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in the introduction to risk and context of the mutual evaluation report under the heading of "Financial Institutions and VASPs", as set out in the instructions for this heading in the Methodology.

[104] Rec. 1, 11, 14, 15, 16, 18, 20, 29, 34 and 40 are under review, see the Technical Compliance Annex.

d) The implementation of preventive measures is generally satisfactory for FIs supervised by the BNB, but remains more variable among those supervised by the FSMA. Business models involving the use of agents, such as certain money transfer operators, present significant risks, which in some cases are not sufficiently controlled. The level of suspicious transaction reports (STRs) is generally satisfactory for CIs, although some still exhibit excessive reporting delays. The concept of beneficial owner (BO) is generally understood, but its determination remains somewhat approximate, particularly for FIs supervised by the FSMA, which often solely rely on the UBO register without cross-checking sources or verifying data consistency.

e) The risk-based approach is generally satisfactory. The BNB and the FSMA have a wide range of off-site and on-site supervisory measures at their disposal. The BNB's off-site supervision is generally adequate. Those of the FSMA focus on the formal compliance of FIs and do not include an analysis of more operational and concrete aspects, which, given the number of FIs supervised and the number of inspections carried out by the FSMA, constitutes a serious shortcoming. On-site inspections are generally thorough and of good quality. However, those carried out by the BNB can take place well after their programming — up to a year later, and sometimes extend over very long period of time —which can reduce their impact and effectiveness. They are insufficient for electronic money institutions (EMI) and, to a lesser extent, payment institutions (PI).

f) In their supervisory actions, the BNB and the FSMA favour an approach based on education, support and knowledge of the sectors supervised, often to the detriment of more restrictive measures. While this approach fosters a constructive relationship with FIs, it limits the deterrent effect of supervision and may unduly prolong situations of non-compliance.

g) The monitoring of remediation plans is generally structured, but relies too heavily on documentary exchanges, with limited use of on-site inspections. Remediation times for FIs supervised by the BNB is sometimes long. Supervisory authorities impose few or no administrative sanctions, which weakens the deterrent impact of the system. Serious administrative measures, such as temporary suspension of activities or deregistration, are applied. However, their use remains sporadic, and some serious breaches have not given rise to any appropriate follow-up, mainly due to what appears to be excessive caution. This lack of adequate response in critical cases, particularly with regards to the BNB, is a concerning weakness in the supervisory mechanism.

h) Since the MiCA regulation came into force on 30 December 2024, no competent authority has been designated to license and supervise virtual asset service providers (VASPs). This constitutes a major loophole in the national AML/CFT framework, creating a major gap in a high-risk sector that is set to grow. The FSMA, which had previously exercised this competence, demonstrated a certain mastery of the sector's issues and ensured effective supervision of provisionally authorised operators.

Key Recommended Actions (KRAs)

Belgium should:

a) Adopt, as soon as possible, a legislative or regulatory framework designating the competent authority for the licensing and supervision of VASPs, in accordance with the requirements of the MiCA regulation (in relation to the technical compliance deficiencies identified in R. 15 - see the TC Annex).

b) Implement the administrative sanction powers of the BNB and the FSMA, in particular by adapting human resources and, where necessary, the legislative framework, to ensure that their action has a truly dissuasive effect. These sanctions should be published, accessible and by name.

Other Recommended Actions

Belgium should:

a) Complement the FSMA's off-site supervisory tools by incorporating more operational off-site supervision, including analysis of sample transactions and compliance files, and ensuring that no category of FIs remains without monitoring of the effectiveness of their system for an extended period of time, while adapting the FSMA's resources accordingly.

b) Develop exchanges on risk issues with FIs in order to strengthen ML/TF risk assessment.

c) Formalise the AML/CFT expertise of inspectors working in this field in order to maintain the BNB's technical expertise and effectiveness in supervising high-risk FIs.

d) Structure a direct and regular dialogue between BNB, FSMA and FIs, and further improve existing cooperation and information exchange mechanisms with the sector, by making them more regular and targeted.

e) Increase the frequency of inspections and ensure that high-risk FIs - including EMIs and PIs - are systematically subject to regular supervision, with a level of intensity commensurate with their risk profile.

f) Extend the cooperation mechanisms between supervisory authorities and other AML/CFT competent authorities, in particular with the police (in the context of detecting illegal activities) and the CTIF (to enhance operational exchanges).

g) Adapt the human and technical resources of the supervisory authorities, in particular for the departments responsible for detecting illicit activities.

h) Improve the planning of BNB inspections to enable the completion of priority inspections for the coming year, including by scheduling a closer inspection cycle for the most exposed FIs and by implementing a system to facilitate the rescheduling of postponed inspections.

i) Provide more structured support to CIs in the implementation of the regulations on basic banking services, which could include the adoption of clear guidelines on the management of high-risk relationships, as well as a monitoring mechanism to prevent unjustified exclusions.

Overall Conclusions on IO.3

Belgium has a broadly sound understanding of ML/TF risks, both among supervisory authorities and the most exposed FIs. This understanding is reflected in particular in supervision that is generally adapted to the identified levels of risk and in the implementation of generally adequate preventive measures for the most at-risk FIs, in particular CIs and *bureaux de change*. Inspections lead to remediation plans that are monitored in a structured manner.

However, two structural limitations relating to FIs and to financial activities with high- ML/TF risks, affect the overall effectiveness of the system. Firstly, since the entry into force of the MiCA regulation, Belgium has not designated a competent authority for the licensing and supervision of VASPs. This represents a major shortcoming in a sector identified as particularly exposed to ML/TF risks. It promotes the illegal exercise of virtual asset activities on Belgian territory and also deprives other European supervisory authorities of a Belgian interlocutor for these activities.

Secondly, the very limited use of administrative sanctions by the BNB and the FSMA, coupled with the almost non-existent or anonymous publication of the measures taken, considerably weakens the deterrent effect of the system. While some serious administrative measures are applied on an ad hoc basis, they are not sufficient to compensate for the overall inertia in terms of enforcement. The impact of supervision is therefore limited, both at the level of individual FIs under supervision, where non-compliance would warrant sanctions, and at the sectoral level, where compliance benefits neither from the deterrent effect of enforcement measures by the supervisory authorities, nor from the guidance that could be drawn from decisions issued by sanctions committee. This gap, which affects all FIs, including major ones such as CIs and PIs, significantly undermines the overall assessment of the effectiveness of the supervisory framework.

These two major structural deficiencies significantly weaken the capacity of the Belgian AML/CFT supervisory system to prevent, detect and deter ML/TF failures.

Furthermore, the evaluation team also notes a significant operational weakness in the FSMA's off-site supervisions, which focus on formal compliance requirements and limits its ability to assess the actual implementation or practical effectiveness of the AML/CFT measures in place. Given the large number of FIs supervised by the FSMA, which include higher-risk entities such as small alternative investment funds (OPCA), this shortcoming is serious, as it may result in these higher-risk entities not being subject to any control of the effectiveness of their systems for long periods of time.

Significant improvements are therefore required.

Belgium is rated as having a Moderate level of effectiveness for IO.3.

Immediate Outcome 3

284. The evaluation team applied the following weighting to assess the implementation of preventive measures by FIs and VASPs: extremely important for credit institutions, payment institutions and VASPs; very important for currency exchange offices (bureaux de change) and life insurance companies; moderately important for lenders and insurance intermediaries, electronic money institutions, collective

investment funds and Bpost; and less important for other FIs. The details of the weighting of each sector are to be found in the Introduction .

285. At the time of the on-site visit, no VASP was registered or approved in Belgium. The implementation of the new European rules governing VASPs (MICA Regulation) was not yet effective, despite the deadline of 30 December 2024, pending the adoption of the measures transposing the amended provisions of Directive 2015/849, as well as the Belgian national measures determining the framework for implementation of the MICA Regulation (see R. 15 in the TC Annex).

3.1. Licensing, registration and controls for FIs and VASPs preventing criminals and associates from entering the market

3.1.1. Market entry controls

BNB

286. The BNB - the European Central Bank (ECB) for credit institutions since the introduction of the Single Supervisory Mechanism (see the Introduction)- is responsible for processing licensing or registration applications and, in this specific context, has mechanisms in place to verify the "fit and proper" character of directors and significant or controlling shareholders. This assessment takes place both at the time of initial licensing and throughout the life of the FIs, particularly in the event of any notifiable changes[105]. This ensures ongoing monitoring and identifies any shortcomings in governance as the institution evolves. The ECB and the BNB share responsibility for the fit and proper assessment of the directors of credit institutions based on their importance, ensuring consistent and harmonised monitoring of financial institutions.

287. The BNB has formalised its fit and proper assessment procedures in various public documents (including the cross-sectoral suitability assessment manual) and internal documents (flowcharts, checklists). The fit and proper assessment is based on several sources, including criminal records and checks with the competent authorities[106], with which the BNB has been in contact in several sensitive cases. In a cross-border context, these verifications are reinforced by international cooperation with foreign counterparts.

288. Formal refusals to approve appointments remain rare: in practice, candidates often withdraw their applications before a negative decision is made, particularly if there are doubts about the candidate's compliance with the fit and proper criteria. For example, in 2019, the BNB reassessed the situation of a director involved in a criminal case abroad. Faced with a draft unfavourable decision by the BNB, he resigned before it was adopted.

289. In addition to these verifications, there is regular and formalised cooperation between the AML/CFT[107] Group and the prudential teams. This coordination strengthens the consistency of AML/CFT measures and promotes an integrated approach to AML/CFT by coordinating prudential fit and proper requirements with AML/CFT regulatory obligations. In addition, the prudential team systematically consults the AML/CFT Group to analyse the AML/CFT framework put in place by institutions applying for licensing, thereby ensuring that new entrants to the financial market are properly assessed, a practice to be encouraged.

290. Finally, since 1 April 2024, a risk-based approach has been adopted for the review of the profiles of senior directors responsible for AML/CFT and/or AML/CFT Compliance Officers (AMLCOs). This targeted

[105] This is the case when a qualifying holding is acquired. A holding is considered qualifying if it represents 10% or more of the capital or voting rights of the bank, or if it allows significant influence to be exercised over the bank.

[106] In particular, the judicial authorities and the FSMA in the event of the first appointment of a prospective director.

[107] The AML/CFT Group is the specialised AML/CFT team with cross-sector expertise in this area within the BNB.

approach allows the level of review to be tailored to the nature and scale of the risks identified, thereby ensuring a proportionate and effective assessment of persons performing these strategic functions.

FSMA

291. The FSMA also has supervisory mechanisms in place to assess the capacity of directors and shareholders exercising control over the entities under its supervision. These inspections are carried out when applications for licensing and registration are submitted, as well as in the event of changes in directors or shareholders requiring prior notification.

292. The FSMA's anti-money laundering centre of expertise *(AML unit*) works with the prudential departments responsible for examining licensing applications. They use the Fit & Proper[108] platform, a cross-cutting procedure[109], the work of a dedicated group[110] and the Fit & Proper Centre of Expertise to harmonise the review of applications. This coordination results in approximately 9% of licences being refused or withdrawn[111]. A reassessment is carried out each time the mandate is automatically renewed or at predetermined intervals for mandates of indefinite duration, which would appear to be adequate.

293. Supervision of access to managerial positions or to the status of controlling shareholder is satisfactory and uses a standardised procedure for all FIs supervised by the FSMA. In practice, entities considered less risky, such as insurance intermediaries, are subject to less stringent supervision.

294. With regard to licensing and registration, the FSMA has recorded a significant number of deregistrations and rejections on fit and proper grounds, particularly among insurance intermediaries. In 2024, 22 of the 36 deregistrations of insurance intermediaries were for fit and proper reasons (not related to ML/TF). Nevertheless, the deregistration rate remains marginal compared to the total number of registered insurance intermediaries (4,835).

VASPs

295. At the time of the on-site visit, no VASP was registered or approved with the FSMA. Since the entry into force of the MiCA regulation on 30 December 2024, no supervisory authority has been designated to license new entities in this particularly risky sector, which constitutes a major shortcoming (see R. 15 in the TC Annex).

296. The FSMA was responsible for monitoring the compliance of VASPs with their AML/CFT obligations when the AML Law was extended in 2022 to providers carrying out virtual and fiat currency exchange activities and offering custodial wallet services. Belgium has introduced a transitional regime for entities that can demonstrate that they were already carrying out these activities in Belgium on a regular and professional basis on 1 May 2022. Entities that notified the FSMA of these activities were entered in a special section of the FSMA register and were required to submit a full application for registration by 1 September 2022. During the period of provisional authorisation, they had to comply with the obligations of the AML Law. The FSMA received 14 applications for provisional authorisation.[112] A number of these applications were withdrawn following notification by the FSMA of non-compliance with, in particular, the conditions of professional integrity of effective directors and/or the sound and prudent management capabilities of the shareholders. These conditions were assessed on the basis of the criteria set by the FSMA

---

[108] This working group was set up by the FSMA with the aim of harmonising the fit & proper assessment for the FIs under its supervision.

[109] This is the "Fit & Proper Manual", which sets out the steps in the procedure for assessing the fit & proper status of a prospective director and the criteria and sources to be taken into account.

[110] It was introduced by the FSMA and must be consulted when there is doubt over the assessment of a candidate's fit and proper status. This centre of expertise keeps an anonymised record of decisions taken in this area to ensure consistent assessment of fit and proper status.

[111] In the *bureaux de change* sector, for example, only one rejection was issued in 2019, mainly due to fit and proper issues.

[112] None of these applications were successful, due to incomplete applications, withdrawals or refusals by the FSMA.

for all FIs under its supervision (see above) and in accordance with a strict approach, given the high level of risk associated with the virtual assets sector.

3.1.2. Detecting and addressing breaches

297. The FSMA's *Périmètre* (scoping) Department, which covers the entire financial sector, is responsible for detecting illegal financial activities. Although its role covers both the prevention and investigation of offences, its work is primarily focused on consumer protection, with the aim of putting an end to fraudulent practices that could cause harm to investors and users of financial services. In this context, the FSMA publishes guidance documents to raise awareness among consumers and stakeholders in the sector. The *Périmètre* team relies on complaints received, its databases and automated tools (such as web scraping) to identify suspicious practices.

298. The *Périmètre* Department's work is not limited to entities supervised directly by the FSMA, but also covers activities subject to BNB licensing, particularly in the area of fund transfers, which is a particularly sensitive issue in Belgium due to cases of cash trafficking and illicit transfers of crypto assets. While concentrating the detection of illegal financial activities within a single department has advantages in terms of efficiency and information flow, it also leads the FSMA to intervene in areas that fall outside its usual remit, for which it does not have the appropriate human and technical resources.

299. One of the main challenges in recent years has been the proliferation of illegal lenders (366 illegal entities detected between 2019 and 2024), which has been made particularly easy by digital channels. In response to this threat, in 2021 the FSMA developed an automated detection tool capable of identifying fraudulent websites offering misleading credit offers. This tool makes it possible to increase the number of sites detected by facilitating the identification of suspicious offers and establishing links with Belgium by identifying elements such as false Belgian addresses, the use of the local language or other location clues. The effectiveness of this tool has contributed to an increase in the number of fraudulent activities detected[113] and warnings issued, which is a significant step forward in preventing illegal activities.

300. When the FSMA detects illegal exercise of a regulated activity, the case is not automatically referred to the public prosecutor's office. The department first assesses the appropriateness of regularisation of the activity in question. If the FSMA has evidence of a criminal offence, it may refer the case to the judicial authorities. Where there are indications of clear fraud, the files are systematically forwarded to the public prosecutor's office and the FSMA proposes that the public prosecutor's office block access to the fraudulent websites. In 2024, the FSMA notified the public prosecutor's office of 33 cases, involving 424 fraudulent websites.

301. Operational limitations remain, particularly in relation to the priority mission of consumer protection assigned to the *Périmètre* Department, which therefore relies mainly on information received from consumers. As a result, certain clandestine practices that are not intended to harm consumer rights, such as informal fund transfers (hawalas) or informal transactions in virtual assets, fall outside its scope of monitoring. These systems are more difficult to detect and are mainly the responsibility of the police, which have more advanced investigative resources but have not put in place proactive detection measures or a systematic detection strategy for these activities (see IO.7). Information on these networks is sometimes passed on via the public prosecutor's office, but the FSMA does not have the capacity to identify these practices independently, which is a persistent challenge for financial supervision and a significant area of risk in the Belgian context.

302. The FSMA is aware of these challenges and has gradually strengthened its cooperation with the CTIF, in particular through the integration of GoAML at the end of 2024, which has improved the exchange

[113] 2018: 1; 2019: 30; 2020: 31; 2021: 80; 2022: 60; 2023: 95; at 30/06/2024: 70

and processing of ML/TF information. The effectiveness of the current system remains somewhat limited in the absence of enhanced cooperation with the police, which would provide access to more advanced investigative tools and better detection of the most opaque illicit financial phenomena. An inter-institutional approach, involving the FSMA, the CTIF, the BNB and law enforcement agencies, would provide a more robust response to the challenges posed by evolving and technologically sophisticated financial crime.

3.2. Actions by the supervisory authorities to identify, understand and promote understanding of ML/TF risks by FIs and VASPs

BNB

303. BNB has refined its approach to identifying ML threats and risks through its Sectoral Risk Analysis (SRA), updated in July 2023. The 2023 SRA, which is more detailed than the 2020 version, includes for the first time an assessment of the risk of TF and incorporates new emerging risks identified in the national ML risk assessment (ML NRA) (see IO.1). Among the trends identified, the emergence of e-IBANs is a major development, facilitating cross-border transactions but also making them more difficult to trace, thereby increasing the risk of misuse. Similarly, increasing attention is paid to the rise of virtual assets, although the BNB has not been at the forefront of this issue, which was the responsibility of the FSMA until 30 December 2024.

304. In addition, the BNB identifies other significant trends in ML risk, such as correspondent banking, which remains an exposed activity as it enables cross-border transactions which involve multiple banks and are often opaque. The impact of Brexit is also a concern, with the arrival on the Belgian market of a greater number of operators from the United Kingdom, which has required an adaptation of the supervisory framework to prevent potential compliance breaches. Finally, digital transformation is seen as a factor bringing about profound change in the financial sector, particularly with the emergence of new operators and services and the growing adoption of practices such as digital onboarding, which poses an increased challenge in terms of checking customer identity and monitoring transactions.

305. These advances in risk identification strengthen the BNB's ability to anticipate risks, but certain limitations persist. The assessment of ML/TF threats is not explicitly included in the SRA, as the BNB has chosen to focus on the internal vulnerabilities of FIs, which are considered more directly actionable. This approach had already been adopted in the first SRA and therefore focuses on correcting compliance failures within FIs rather than on a quantitative assessment of the external threat.

306. While this approach provides a better understanding of the vulnerabilities specific to the sector, it remains incomplete in the absence of a more integrated threat analysis that also takes into account external developments and criminal modus operandi. Furthermore, the SRA does not establish a clear link between the risks identified and the types of FIs or services concerned. This limits its operational scope and makes it difficult to tailor supervision to the specific risk level of each segment. As a result, although well structured, the SRA remains largely theoretical and not particularly operational.

307. Certain risks, such as correspondent banking, are well identified, but their actual impact in Belgium is not clearly explained, which limits the relevance of mitigating measures. Cyclical risks, such as those related to Brexit or FinTechs, are only addressed generally, without specific figures or concrete examples to assess their real impact on ML/TF risks. For example, the section on money transfer services, which is considered a high-risk activity, contains approximations and does not provide sufficient detail on the specific money laundering patterns identified through the inspections carried out. On the other hand, certain issues, such as the use of cash, are analysed in greater depth and better illustrated, demonstrating

that a more factual and documented approach is already being implemented in some areas and should be extended to others.

308. Better integration of data from the BNB's AML/CFT supervisory actions and information reported by FIs would make this assessment more concrete and useful. While the formalisation of a framework for exchanges between the BNB and the CTIF in 2019 represents progress in light of the conclusions of the FATF's 2015 Mutual Evaluation, greater cooperation with the CTIF, law enforcement agencies and other competent authorities, particularly on virtual assets and cross-border financial services, would improve anticipation of risks and the adjustment of supervisory measures. Such a development would ensure a more dynamic and responsive approach, better aligned with the realities on the ground and the proven challenges in the area of AML/CFT.

309. As part of its supervisory approach, the BNB carries out horizontal thematic actions aimed at deepening its understanding of FI risks. A notable example of this approach is the action taken on de-risking, which followed the publication in February 2022 of a circular incorporating the AML/CFT issues related to this problem. This type of initiative provides a structured framework for FIs and clarifies their expectations. A similar approach was adopted for asset repatriations (often involving large amounts), with a horizontal action carried out off-site in 2020 to assess the due diligence measures applied by FIs active in wealth management and the issue of single-premium life insurance contracts. This analysis led to the publication of a circular in 2021 formalising the expected best practices. In 2024, a horizontal action specific to correspondent banking was also carried out, in line with the BNB's desire to assess the specific vulnerabilities of this activity in greater depth.

310. However, the BNB could strengthen its understanding of ML/TF risks through more frequent and structured exchanges directly with FIs. Certain risks, such as those related to high-risk situations in the context of basic banking services, are insufficiently identified and analysed, limiting the effective support provided to FIs in managing their risks and adjusting their preventive measures. In this regard, despite the obligation for FIs to inform the BNB of updates to their overall risk assessments, this is not accompanied by a more regular dialogue focused on risks.

311. The BNB requires each FI under its supervision to provide it with its updated assessment of risk(EGR) on an annual basis. The BNB conducted a horizontal review of these EGRs in 2018-2019. This was followed by the publication of a communication specifying the BNB's expectations in this respect (January 2020).

312. The BNB develops risk profiles for each FI and assigns them a risk score based on a periodic AML/CFT questionnaire and the AMLCO report, as well as any events that may have affected the FI during the period under review. These elements are also used for updates. Newly licensed FIs are only assigned an individual profile after these elements have been submitted for the first time, which may lead to a delay in the formal assignment of their risk score. This delays the integration of these entities into the risk-based supervisory framework, even though relevant information has already been collected and analysed during the licensing process. In the absence of an anticipated initial risk score, initial supervisory actions may not be well aligned with the entity's actual level of risk.

313. The BNB considers that the periodic reporting obligations of FIs, in particular the AML/CFT questionnaire and the updating of the EGR, constitute a significant administrative burden for the FIs under its supervision. It therefore provides for the possibility of exemption at the request of the FI concerned. This exemption (which at the end of 2024 concerned 17 FIs out of the 192 supervised by the BNB, see section 3.5) allows eligible institutions (FIs in the lowest risk categories, medium/low or low risk) not to submit these documents, with the exception of the AMLCO report, which may, however, be simplified. This procedure is part of a specific approach applied to certain FIs, pooled together and subject to lighter supervision, which would appear to be appropriate subject to regular reassessment (see section 3.5).

FSMA

314. The FSMA's first ML/FT SRA was finalised in September 2024 and uses a clear, two-step methodology (inherent risk followed by residual risk) based on a variety of relevant sources (both national and international). It is based in particular on the results of supervision carried out between 2018 and 2023 and on the ML/TF threat assessments described in the ML/TF NRAs. Although the SRA was finalised late, it provides a good quality analysis, identifying risks by sector in a detailed and comprehensive manner. However, the threat, particularly in terms of TF, is not assessed for several types of entity (e.g. mortgage lenders, asset management companies, collective investment scheme managers), which weakens the reliability of the overall analysis and impacts the reliability of the final rating for these entities.

315. In 2022, the FSMA formalised its cooperation with the CTIF regarding the transmission of suspicions of ML/TF revealed during inspections (see IO.6). This is a step towards better risk assessment in the sectors supervised. However, although exchanges with the CTIF are direct, they remain insufficiently developed, which limits alignment between the NRA and sectoral analyses. As a result, currency exchange offices are considered high risk in the FSMA's SRA, while the NRA, based on a different methodology and external sources not available to the FSMA, classifies them as moderate risk.

316. The FSMA uses risk assessment models (an automated model or a semi-automated Excel model based on five risk categories) to assign an individual risk score to each FI. These assessment methods differ depending on the sectors supervised, allowing them to be adapted to the specific characteristics of each sector. However, the lack of convergence between these approaches limits the ability to obtain a comprehensive and consistent view of the risks. The work in which the FSMA is involved at European level aims to remedy this fragmentation in methodology.

317. Individual risk assessments are mainly based on periodic questionnaires sent to FIs via FiMiS, a tool that enables automated processing. For insurance intermediaries and social lenders, including those that no longer grant new loans, the risk profile is reviewed every three years. In the intervening years, a sample of around 3,500 to 4,000 entities (i.e. 80% of the 5,000 existing entities) receive a questionnaire, including in particular the major players and those assessed as presenting a risk. This approach, although based on the number of entities concerned rather than a strict risk-based approach, would appear to be appropriate.

318. The FSMA uses these periodic questionnaires to assess, among other things, the implementation of ML/TF risk mitigating measures by FIs. However, these responses are only subject to occasional monitoring, which limits the FSMA's ability to monitor changes in residual risk in a consistent manner.

319. The FSMA does not require the FIs under its supervision to send it their updated ORAs, which prevents it from ensuring that the risks are properly understood. In principle, off-site compliance inspections include an analysis of the FI's ORA. FSMA's understanding of the risks faced by FIs varies greatly and is sometimes insufficient, making a more systematic analysis of risk assessment necessary, rather than waiting for an off-site compliance inspection to be carried out.

320. FSMA also relies on AMLCO reports to identify and monitor ML/TF risks in its sectors. However, although these reports are required annually, they are not systematically analysed, thus limiting their contribution to the understanding of risks. In 2024, only 275 reports were reviewed for 5,550 FIs under supervision, limiting the FSMA's ability to identify trends and adjust its supervision in line with the vulnerabilities detected. To remedy this, the FSMA plans to develop an automated tool, inspired by FiMiS, to improve the use of this data and strengthen its risk-based approach.

321. The risk score generated by the risk analysis tool can be adjusted based on other factors, such as the results of inspections, information received from other authorities (in particular the BNB and the CTIF), or data from the press. Risk and mitigation factors are weighted according to their importance and relevance. This flexible methodology would appear to be well suited to ensuring a more detailed risk assessment tailored to the realities on the ground.

322. In 2023, the FSMA applied for the first time a procedure for FIs that did not respond to their periodic questionnaire, including suspension and then removal from the register in the event of non-response after formal notice. Although time-consuming due to the large number of FIs concerned (3,939 in 2023), this process proved to be effective in encouraging FIs to comply with this obligation.

323. With regard to VASPs, the FSMA demonstrated a good understanding of the risks associated with these entities, albeit based on limited activities in this area (see introductory paragraph to IO3 and section 3.1 above). The FSMA included VASPs in its 2024 SRA, without however assessing the residual risk associated with this activity, and based part of its expertise on the examination of applications for listing in the VASP register during the transitional period (see above). These activities enabled it to gain a better understanding of the specific business model of each VASP applicant and to better grasp the technological and legal issues related to virtual assets. The FSMA also benefited from exchanges and training with the judicial police. The absence of active service providers in this area and the uncertainties surrounding the future supervisory authority for VASPs in the country do nothing to help maintain advanced expertise in a field that requires constant updating of technical knowledge that is rapidly evolving.

SPF Finance - Treasury

324. The product-specific risk analysis distributed by Bpost, carried out in 2020 by SPF Finance/Treasury, produced appropriate conclusions, although the depth of the analysis remained limited. In particular, this analysis concludes that there is a significant residual risk for payments to third-party accounts, payments to government postal accounts and Bpaid prepaid cards, mainly due to the use of cash, which is central to these financial products and services. The use of cash is also identified as the main risk to which Bpost is exposed, which would appear to be relevant and is clearly identified in the NRA. However, the different types of service offered by Bpost in relation to payments into third-party accounts are less clearly identified in the NRA. The risks associated with Bpaid prepaid cards are considered by the NRA to be lower due to the relative lack of anonymity, although this circumstance is considered to have no impact on risk by the risk analysis of Bpost products. The TF risk associated with these cards is nevertheless identified by both analyses. The risks associated with the substantial amounts that can be loaded onto each card (EUR 8,000, with each customer able to hold three cards) and the possibility of withdrawals from foreign ATMs do not appear to be sufficiently identified in the product risk analysis carried out by SPF Finance/Treasury.

325. Quarterly meetings are held between SPF Finance/Treasury and Bpost to discuss risks and trends in this area. Annual discussions are held with CTIF on trends and new types of ML/TF.

3.3. FI and VASP understanding of existing and evolving ML/TF risks

FIs under BNB supervision

326. FIs supervised by the BNB generally demonstrate a good understanding of ML/TF risks, particularly those most at risk, namely credit institutions (CIs) and payment institutions (PIs) and, to a lesser extent, electronic money institutions (EMIs). However, this understanding varies more among certain FIs that have adopted innovative business models, particularly those using virtual IBANs, as the BNB's inspections have also found. In these cases, commercial imperatives seem to take precedence over ML/TF risks, which remain insufficiently controlled. These products enable customers located in countries with varying AML/CFT regulations to make payments via a Belgian IBAN, giving them the appearance of a presence in the EU, which represents a high inherent ML/TF risk.

327. FIs' understanding of ML/TF risks is based on several sources, such as the SRAs, CTIF's annual report and the internal assessment they are required to carry out. However, this understanding remains partial. Due to their limited dissemination (see IO.1), ML and TF NRAs are not well known by FIs, which limits their ability to develop a comprehensive view of external threats. Furthermore, the BNB's current approach in its

SRA, which focuses on internal vulnerabilities rather than on the explicit assessment of external threats (see section 3.2), further reduces the scope of a comprehensive and integrated view of ML/TF risks and hinders FIs' understanding of the overall context of their risks.

328. The BNB verifies understanding of the risks by asking FIs to submit their updated internal assessments annually, except for exempt entities (see 5.2.1). Some FIs go beyond analysing existing risks and identify risks that are insufficiently or not at all covered by the SRA, such as high-risk situations in the context of basic banking services for businesses, correspondent banking, or certain high-risk customer profiles (e.g. fake bookshops, betting centres). This capacity for independent analysis demonstrates that the FIs supervised by the BNB are, on the whole, capable of identifying and assessing their own risks.

329. Finally, some FIs consider that the SRA remains too theoretical and not very practical (as it is not very operational), and highlight the lack of sufficiently concrete analyses to help them implement their AML/CFT measures effectively.

FIs under FSMA supervision

330. The FSMA notes an increase in the number of FIs that have individually carried out an ORA and an improvement in their quality: the ORAs also appear to be better documented and regularly updated. However, in general, the FIs under FSMA supervision have varying levels of understanding of the risks. *Bureaux de change*, for example, do not seem to have a good understanding of their risks, which compromises the effectiveness of their vigilance measures.

331. Supervision shows that insurance intermediaries have a more variable understanding of ML/TF risks. In 2024, 74% of them had carried out an ORA, but some shortcomings may persist, particularly in their ability to identify, document and update these risks, despite support from the FSMA and their professional association, which compromises the effectiveness of their AML/CFT measures.

332. Other categories of FI do not yet seem to have fully identified all the risks to which they are exposed. For example, one lender had to belatedly regularise a significant number of STRs involving unsubstantiated early repayments and cash payments via third parties, in particular via Bpost. Similarly, the risks of TF via consumer loans remain underestimated by some of these operators, highlighting the need for greater awareness and monitoring in these sectors.

333. Furthermore, the FSMA does not systematically require FIs to update their ORAs, which raises questions about their ongoing understanding of risks and also reduces the FSMA's ability to ascertain the actual level of understanding of risks by these players, with an indirect impact on genuinely risk-based supervision.

SPF Finance – Treasury

334. Bpost carried out a risk assessment with the help of a third-party auditor in 2021. This assessment is reviewed annually and is also discussed with the Treasury.

3.4. FI and VASP understanding and compliance with AML/CFT obligations and mitigating measures

3.4.1. Customer due diligence, record keeping, BO information and ongoing CDD

335. The analysis of the results of FI supervision, on one hand, and interviews conducted during the on-site inspection, on the other hand, showed that FIs generally have adequate customer due diligence measures in place at the time of entering into the business relationship and on an ongoing basis during the relationship. In the banking sector, FIs apply due diligence measures when *entering into business*

relationships and monitor transactions appropriately. CIs sometimes adopt a cautious approach, limiting their exposure to risk by refusing certain customers. There is strong reluctance towards transactions involving virtual assets. De-risking practices exist, particularly for categories of customers considered high-risk, such as diamond dealers. In response to this trend, the public authorities reacted by imposing an obligation to provide basic banking services, initially in 2003 for individuals and then extended to legal entities in 2021, in order to limit exclusion from the banking system.

336. With regard to *digital onboarding*, the FIs are generally aware of the specific challenges and requirements on the subject. PIs and EMIs routinely develop remote business relationships using identity verification tools. However, these processes often involve the use of numerous external service providers offering advanced technological solutions (e.g. facial recognition), thereby increasing the risk of faults. PIs and EMIs also frequently use agents who are in direct contact with customers. For these agents, PIs and EMIs seek to limit risks by imposing strict procedures, making all transactions conditional on compliance with these procedures. However, these agents remain exposed to document fraud, particularly due to the optional nature of tools for verifying the authenticity of identity documents. In addition, their large number and their ability to work for several payment institutions increases the vulnerability of the model, making it more difficult to monitor the quality of the checks carried out.

337. In the insurance sector, when an insurance company uses regulated insurance intermediaries, due diligence is often delegated to them, as they are the first point of contact with the customer. This outsourcing can create vulnerability in this sector, which is exacerbated by shortcomings in the application of due diligence measures by intermediaries, despite the 'sectoral code on the distribution of financial products' drawn up in consultation with Assuralia,[114] and by the regular use of non-reporting agents. To address these shortcomings, some operators have introduced dual supervision involving both the intermediary and the insurer. However, this approach carries the risk of diluting responsibilities, as each party may rely on the other to assume the burden of supervision.

338. Due diligence measures are applied more inconsistently among FIs supervised by the FSMA. While some currency exchange offices have strengthened their compliance thanks to FSMA supervision, others remain deficient, particularly with regard to the distinction between occasional customers and business relationships, customer scoring and data retention. Among insurance intermediaries, shortcomings persist in terms of customer knowledge and document retention. Asset management companies (alternative OPCAs/OPCVMOPCVM) find it difficult to define the notion of customer, and the application of procedures remains variable. It has not been possible to assess the implementation of their ongoing CDD obligations by "small" alternative OPCAs, which present higher risks.

339. Some business models, such as those of insurance intermediaries or lenders, rely on non-reporting agents, which complicates the implementation of due diligence obligations. Intermediaries, acting on behalf of insurers, are not always fully aware of their responsibilities. In general, FIs do not enter into business relationships without being able to apply due diligence measures. Good practice is observed among some payment institutions, currency exchange offices and lenders, which use tools to detect false documents, and this could be extended to other sectors.

340. Bpost implements due diligence measures tailored to its customer base, which consists solely of individuals acting for their personal needs, and to its operations, which are limited to Belgium. Bpost refuses to enter into a business relationship if these measures cannot be implemented. Transactions are constantly monitored using the Fiserv tool. In addition, if the validity date of the document provided for identity verification has expired, the customer cannot carry out any transactions until a valid document has been provided. A limit of EUR 1,000 is applied to each cash transaction (and EUR 2,500 by bank card), with a monthly limit of EUR 2,000. These limits are an improvement on the 2015 MER. However, shortcomings

[114] The Belgian professional association of insurance companies

have been identified by Bpost's independent audit function with regard to the implementation of preventive measures and financial sanctions such as embargoes. Topping up the Bpaid card with cash has been subject to stricter conditions since 2022. However, the storage limit remains high (EUR 8,000) and a customer can have up to three cards.

341. The *identification of BOs* is generally based on the regulatory threshold of 25% of the capital of a legal entity (direct or indirect). Among the FIs under FSMA supervision in particular, and mainly among some of the smaller insurance intermediaries, the definition of BO is often poorly understood, being limited to the mere holding of shares without taking control into account. Most of these FIs include this criterion as a starting point in their procedures, without always taking into account other forms of effective control, such as the ability to appoint or dismiss directors. Consistency checks (verification of corporate purpose, signing authority, etc.) are not systematically included. Very few entities carry out an in-depth analysis of the holding chain in order to identify the natural person exercising effective control. In addition, the level of documentation required varies significantly from one entity to another.

342. With the exception of large FIs that have their own sources of information, most FIs use the BO register as their main source of information for verifying the identity of beneficial owners. However, frequent discrepancies are found between internal data and the data recorded in this register, and are generally reported to SPF Finance/Treasury (see IO.5). In some cases, especially for FIs under FSMA supervision, consultation of the register is the only means of identification, which limits the reliability of the analysis and hinders the detection and reporting of any discrepancies.

343. The identification of BOs is particularly difficult in complex structures, especially those involving foreign entities. The documents collected are systematically retained. If a customer or their BO cannot be identified, the institution will not enter into a business relationship. However, discrepancies with the BO register do not have a direct impact on this relationship, which would appear to be proportionate.

344. With regard to *ongoing CDD*, various CIs use AI to monitor and analyse transactions, particularly cash transactions or potential misuse involving legal persons. The BNB supports this development by organising workshops on AI. Credit institutions developing private banking activities adequately monitor fund repatriation transactions, particularly with regard to the origin of these funds. Shortcomings in monitoring persist among insurance intermediaries and lenders.

345. The BNB identified cases of non-compliance with the requirements on information accompanying fund transfers, including serious breaches at two credit institutions in Belgium in the context of Brexit. For PIs and EMIs, transaction monitoring varies according to the business model adopted, in particular depending on the involvement of agents or marketing under white labelling. A common feature emerges, namely the outsourcing of transaction monitoring and the extensive use of subsidiaries or branches located outside Belgium to prepare STRs for the CTIF, which, in the absence of real involvement by the FI located in Belgium, may increase the risk of STRs being sent that are irrelevant, automated or of poorer quality because they are prepared by staff who only have a theoretical knowledge of the Belgian context, thus complicating internal control. When agents are involved, their monitoring is based on strict procedures. However, in the context of fund transfers, these measures remain insufficient to ensure effective traceability of the origin of funds for a large proportion of transactions, thus exposing the system to significant vulnerabilities.

346. In the interests of profitability and speed, some payment institutions fragment fund transfers to avoid reporting requirements. By circumventing AML/CFT reporting requirements for information accompanying these transactions, these payment institutions significantly weaken the effectiveness of their transaction monitoring systems. This model exposes these PIs to an increased risk of non-compliance, thereby compromising the objectives of financial regulation and the prevention of illegal activities.

3.4.2. Enhanced or specific measures

347. The FIs under BNB supervision generally have a good understanding of the concepts of PEP and high-risk third countries, with appropriate measures in place, including the setting of acceptance limits for transfers from certain countries by certain banks. However, the BNB has identified shortcomings in the hierarchical approval process when establishing or maintaining business relationships with customers residing in high-risk third countries. By contrast, enhanced transaction monitoring is generally well implemented.

348. For FIs under FSMA supervision, the definition of PEPs often remains vague, sometimes excluding close relations or, conversely, extending the definition excessively, leading to the unjustified application of enhanced due diligence measures. The detection of PEPs still relies mainly on manual searches or self-certification, due to the lack of automated screening tools. Although the measures applied are generally appropriate, they sometimes need to be adjusted to the size of small FIs. The number of PEPs among customers is perceived as low, but insufficient understanding of the concept of PEPs may lead to an underestimation of their number, resulting in inadequate due diligence and, in some cases, excessive mistrust, which encourages de-risking. Similarly, the low number of customers residing in high-risk third countries may partly reflect ongoing confusion between these countries and those under embargo or blacklisted. Finally, only 61% of insurance intermediaries that have carried out an ORA apply enhanced measures to high risks, revealing a lack of consistency in risk management.

349. Bpost has a customer base of PEPs, which are detected using an automated tool and systematically classified as high-risk. The AML compliance team decides whether or not to accept these customers. The list of high-risk countries is updated every month. A customer residing in such a country is identified as presenting a higher risk. Bpost's transactions do not appear to be particularly exposed to this risk, as operations are limited to Belgium. Nevertheless, Bpaid cardholders can withdraw the cash loaded on their cards from an ATM located abroad, which constitutes a risk that does not appear to be sufficiently mitigated.

3.4.3. AML/CFT reporting obligations and tipping off

350. The FIs under BNB supervision have a good understanding of their reporting obligations (96% of STRs originate from FIs, almost equally divided between credit institutions and payment institutions) – see box below. However, in the absence of legal clarification or precise guidance on reporting deadlines, these vary considerably, ranging from 1 to 90 days (see c 20.1).

Table 3.1. FI reporting activity (2019-2024)

	2019	2020	2021	2022	2023	2024
Credit institutions	11 237	17 678	21 624	28 379	40 129	39 894
Payment institutions	5 814	62 63	16 016	16 425	25 141	41 938
Electronic money institutions	90	654	774	520	5 442	2 733
Life insurance	309	661	749	1 172	2 374	1 244
Mortgage lenders	83	166	671	1 188	699	652
Consumer credit lenders	132	151	117	183	244	228
Bpost	1 470	897	1 082	583	643	631
Currency exchange offices	117	106	23	82	44	37
Investment companies	2	70	10	19	13	7
Investment management and investment advisory companies	-	3	7	12	10	6
VASPs	-	-	-	10	7	0
Insurance intermediaries	4	5	6	4	3	5

Source: CTIF

351. Some CIs and EMIs are major contributors of STRs to the CTIF because of their location in Belgium, but a large proportion of these STRs are redirected to other European FIUs with which suspicious transactions have closer links. The CTIF's frequent collaboration with its European partners improves the quality and speed of STRs.

Box 3.1. Factors explaining the increase in STRs from CIs, PIs and EMIs

- For CIs, this is explained, among other things, by a new approach to and organisation of the CI compliance function and, more generally, by retrospective reviews ("lookbacks") initiated by CIs at the request of the BNB on various topics such as money mules and correspondent banking. The BNB circular of 8 June 2021 on the repatriation of funds from abroad also had an impact on CIs and life insurance companies. This measure led to increased due diligence and, as a result, to an increase in reports of financial flows considered atypical or suspicious.
- The PI sector has undergone significant changes following Brexit, with several payment service providers benefiting from the European passport moving to Belgium. This expansion has led to an increase in the volume of transactions processed in Belgium and, in turn, to an increase in STRs.
- Finally, in the EMI sector, a remediation plan implemented at the instigation of the BNB has strengthened the reporting obligations for at least one of the operators concerned, thereby contributing to the increase in the volume of STRs originating from this sector.

352. For FIs under FSMA supervision, reporting times remain excessive. The periodic questionnaire does not contain any questions on this subject, but checks carried out by the FSMA reveal that some STRs are submitted two to three months after the detection of a suspicious transaction (see c 20.1). Feedback from the CTIF indicates that the overall quality of reports is improving, although customer information is sometimes incomplete. The CTIF also notes very low reporting activity among insurance intermediaries. Among the FIs most at risk, it should be noted that in 2022, one bureau de change was responsible for the majority of STRs received (60 out of 82), which contributed to pushing up the overall figures for that year. However, some other bureaux – particularly those that had been inspected by the FSMA – had significantly reduced their reporting activity. In its feedback to the FSMA in 2023, the CTIF also noted the insufficient quality of the reports issued by this sector. In response to these findings, the FSMA launched a thematic supervisory initiative in 2023 focusing on the reporting activity of currency exchange offices (see section3.5). The GoAML tool already appears to be improving the quality of reports, but some operators have yet to finalise their registration. In 2024, entities under FSMA supervision accounted for only 0.8% of the STRs sent to the public prosecutor by the CTIF. Reporting activity is mainly carried out by lenders and bureaux de change, while other sectors report very little.

353. The number of STRs sent by Bpost to the CTIF has fallen (1,082 STRs in 2021, 583 STRs in 2022, 643 STRs in 2023), reflecting the decline in its activity due to the termination of its collaboration with a major European public entity at the beginning of 2020 and the new rules imposed on payments to third-party accounts. The transmission time is around 30 days, which remains quite long. The CTIF forwards 6 to 8% of these STRs to the public prosecutor. The quality of the STRs would appear to be satisfactory and they are sufficiently documented. Certain information, such as the originator and their account number in the case of fund transfers and the postcode of the post office where the transaction was carried out, is not yet systematically provided. The difficulty or even impossibility of determining the origin of the funds, due to the business model, often gives rise to suspicion.

354. The ban on disclosure is well understood and applied.

3.4.4. Internal controls, procedures and audits to ensure compliance

355. CIs generally have structured and effective internal controls. However, there are some persistent shortcomings: for FIs belonging to a European group, particularly those established in Belgium after Brexit, the conduct of due diligence checks by intra-group entities is sometimes poorly supervised, which can weaken the control system. Small and medium-sized FIs often lack clarity in the organisation of the three lines of defence, and have limited resources. This can lead to overlapping responsibilities: for example, the second line takes on tasks that fall within the remit of the first line, which results in the loss of one level of supervision.

356. Among the entities under FSMA supervision, a lack of internal control is a recurring weakness, noted in particular during on-site inspections.

357. Bpost has first and second level internal controls.

358. The *audit function* is generally adequate in CIs, although it is sometimes affected by the same shortcomings as the internal control systems mentioned above (particularly in international groups or small FIs). However, the internal audit of credit institutions is considered effective. Belgian regulations stipulate that the independent audit function depends on the nature and size of the FI (R. 18 in the TC Annex), which allows for some flexibility in how this function is organised but requires that a minimum mechanism be in place, which does not seem to be the case in all small or less well-resourced FIs under FSMA supervision. Bpost has an independent audit function which appears adequate.

3.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

359. The evaluation team did not identify any legal or regulatory obstacles to the implementation of AML/CFT obligations and mitigating measures.

3.5. Supervision and monitoring of FIs and VASPs by supervisory authorities using a risk-based approach

BNB

360. Since January 2020, the BNB has applied a risk-based supervisory policy to monitor the implementation of AML/CFT measures at 209 institutions, including the four largest banks representing 87% of assets. Although late, this approach has strengthened the maturity of the system thanks to a four-pillar framework and risk scoring. Created in 2016, the AML/CFT Group has almost tripled its staff to 18.4 FTE in 2024 (including 12.95 FTE dedicated to off-site supervision), with a ramp-up in off-site supervision and a tripling of resources dedicated to inspection (from 3 FTEs in 2016 to 10.5 FTEs in 2024). These developments are a clear improvement on the findings of the 2015 MER. The BNB does not have inspectors dedicated exclusively to AML/CFT; all inspectors can work on all of the BNB's supervisory areas. AML/CFT is the primary or secondary area of expertise of several inspectors, but this has not yet been formalised in order to ensure its continuity, development and the maintenance of the quality of inspection reports.

361. The BNB deploys a wide range of AML/CFT supervisory tools, both off-site and on-site, including thematic reviews, inspections, flash missions and special audits entrusted to statutory auditors. Each of these tools has a specific objective:

- thematic reviews enable the BNB to take stock of practices across a sector in a specific area;
- inspections provide comprehensive, detailed and in-depth knowledge of the effectiveness of an FI's AML/CFT system;

- “flash” missions aim to obtain targeted information on the effectiveness of an FI’s AML/CFT system, often as part of the follow-up to a remediation plan; and finally
- special audits entrusted by the BNB to the approved auditor provide a more accurate picture of the effectiveness of the measures in place as part of the follow-up to a remediation plan.

362. These control tools are used appropriately and with a view to improving FI compliance. Off-site inspections are based, among other things, on an analysis of the AML questionnaire, EGR, AMLCO annual report, information received from the CTIF, as well as interviews and targeted tests (sample client files, monitoring alerts, review of internal procedures). For FIs with major deficiencies, an intensive monitoring procedure is put in place, allowing for close supervision, an approach that is considered effective.

363. At the end of each year, the AML/CFT Group draws up a list of FIs eligible for inspection for the coming year, based on their level of residual risk, the SRA, and internal (from off-site supervision) and external information, among other factors. Since this list of eligible FIs is, by definition, longer than the number of inspections that can actually be carried out in the coming year, the AML/CFT Group also ranks the desired inspections in order of priority. This list is discussed with the inspection teams within the prudential departments. However, the final schedule is decided by the inspection teams, in consultation with the AML/CFT Group. The number of inspections actually carried out depends on the resources allocated to AML/CFT inspections by the BNB Management Committee. Due to the need to set priorities, around half of the eligible inspections are rejected because the number of requests far exceeds the available inspection capacity. This circumstance may result in the postponement of eligible inspections by the AML/CFT Group, with some inspections deemed to be of lower priority being postponed for one year or more. In this case, and if deemed appropriate, the AML/CFT Group will incorporate specific supervisory actions into its off-site supervision programme. No margin is provided for additional inspections, thereby limiting the responsiveness and flexibility of the system. The emergence of a critical risk or a desired change to the inspection plan can only be incorporated by postponing an inspection included in the inspection plan (this was the case for the first two de-risking inspections).

364. Supervision of the information accompanying fund transfers, which is integrated into inspections, is considered adequate. However, cash-related risks do not appear to be sufficiently taken into account in the planning of inspections for certain exposed institutions (as identified in the BNB’s NRA and SRA, in particular CIs).

365. In 2023, the BNB supervised 183 of the 209 institutions through off-site inspections, covering 100% of high-risk entities and 85% of medium-high risk entities. This coverage appears to be robust and targeted, in line with effective risk management, ensuring satisfactory monitoring. Off-site actions and inspections may lead to administrative measures, severe or otherwise, or to sanctions, giving the AML/CFT Group greater flexibility and responsiveness. However, the real impact of this monitoring depends on the ability to intervene and respond to problematic cases. In practice, only inspections with the lowest score (4/4) or with a score of 3/4 and at least one critical recommendation are discussed with a view to the possible application of an administrative measure, severe or otherwise, and/or a sanction. In practice, the majority of administrative measures, severe or otherwise, were imposed on FIs on the basis of a prior inspection.

366. Inspections carried out by the BNB are lengthy and require significant resources. Their average duration is 8.3 calendar months,[115] with some lasting more than a year and others being shorter (3 to 6 months). They involve 2 to 4 inspectors and represent a significant time commitment. The quality and detail of the inspection reports are to be commended: they are based on observations, ratings and recommendations, with a criticality rating (“critical”, “high”, “medium”), and are scored out of 4 (4 being

[115] This duration takes into account the unforeseeable circumstances associated with inspections and includes five “full programme” inspections of large banks carried out between 2020 and 2022.

the lowest score). Thanks to their level of detail and clarity, they are a key tool for the BNB and FIs, facilitating the understanding of shortcomings and the implementation of effective corrective measures.

367. The BNB applies a lighter off-site supervision regime for certain FIs classified as medium/low risk or low risk, which are pooled together. Three members of the AML/CFT Group are primarily assigned to the supervision of these 35 FIs (as of 31 July 2024), 14 of which are exempt from certain reporting requirements to the BNB (see section 3.1). This system is designed to respond when necessary and to verify the relevance of the risk score every two to three years. This approach is subject to regular assessment to ensure that this lighter supervision remains adequate, which the BNB undertakes. One case illustrated this need: a Belgian branch of a PI authorised in Greece, initially classified as purely commercial, was ultimately identified as involved in establishing business relationships, leading to an adjustment of its supervision by the BNB.

368. Exchanges between the BNB and its counterparts, particularly in Europe, are regular and appropriate for AML/CFT supervision of groups. The active participation of the CTIF in oversight boards, with the sharing of analytical information, is good practice.

369. The monitoring of entities authorised post-Brexit is considered effective, with several inspections carried out and corrective measures applied. The EMIs and PIs inspected were appropriately selected from among those presenting the highest risks and/or materiality. However, supervision of EMIs and PIs remains insufficient: only one EMI was inspected in 2019, compared with 13 in 2020 and 7 in 2023; for PIs, only five inspections were carried out between 2020 and 2023 (one in 2020, two in 2022 and two in 2023), out of a total of 53 PIs. This low coverage rate, despite the risks presented by these categories of FIs, increases the risk of prolonged non-compliance.

FSMA

370. In general, the FSMA has strengthened its risk-based approach with several areas of progress since the 2015 MER: introduction of a periodic questionnaire and individual risk assessments (since 2018), creation of an AML/CFT centre of expertise (2022), formalised cooperation with the CTIF (2022) and other European authorities (from 2019), and publication of its first SRA (2024).

371. The AML centre of expertise handles a reasonable number of cases per year. The annual supervision plan follows a risk-based approach, incorporating the SRA and the documents submitted by the FIs. The FSMA combines off-site and on-site supervision, with the latter mainly carried out in the most high-risk sectors. Off-site supervision includes interviews with the AMLCO, review of the AMLCO's annual reports, analysis of audit reports and mandates given to statutory auditors, and a spot check of responses to periodic questionnaires on the implementation of risk mitigation measures. Thematic inspections covering several FIs on specific aspects may be carried out (e.g. an analysis of the monthly reports sent by all bureaux de change). Some of these inspections are primarily aimed at improving the FSMA's understanding of a sector.

372. The FSMA may also decide to carry out an off-site inspection of the existence and adequacy of policies and procedures. These more in-depth inspections aim to assess the existence and completeness of a financial institution's AML/CFT system (see section 3.6).

373. These off-site inspections, which are formal, appear to be appropriate for the purpose of gaining a better understanding of a sector or for ensuring the existence and completeness of policies and procedures. However, given the large number of FIs supervised by the FSMA and the relatively limited number of inspections scheduled, the formal nature of these off-site inspections limits their effectiveness. Their impact is reduced by the absence, in some instances, of more operational data, such as analysis of transactions and customer files, which would enable a concrete assessment of the implementation of risk mitigating measures. Off-site controls are quick with a 1-2 month turnaround time for analysis and 2-3

months for remediation. Inspection reports are deemed to be of good quality, providing sufficient level of detail to enable the FI to understand its deficiencies and improve.

374. The FSMA has AML inspectors who, together with the AML centre of expertise, carry out on-site inspections. These inspections, which may be announced or unannounced, take one to two days, rarely longer, with an in-depth analysis and cross-checking phase upstream and downstream. They assess the formal compliance of policies and procedures and their effectiveness by examining a selection of customer files and transactions. However, they do not always check whether the mitigating measures implemented are actually appropriate for the risks presented by the FI.

375. The FSMA has the flexibility to carry out ad hoc inspections, i.e. unscheduled inspections, which may be conducted on or off-site, announced or unannounced, as required (e.g. following an off-site inspection, an event or press articles). Its inspection procedure is quick and effective, particularly for currency exchange offices, for which the inspection plan would appear to be appropriate: over the years 2023-2024, all eight currency exchange offices were inspected. These on-site inspections followed a thematic action carried out in 2023 on reporting activity. They revealed an initial improvement in the quality of STRs, which are now based on concrete analyses rather than quantitative thresholds. However, the findings for three currency exchange offices still point to insufficient or late reporting.

376. Certain categories of FIs are not sufficiently supervised, particularly through on-site inspections (see table below). This is particularly the case for managers of small OPCAs, which are identified as being of the highest risk in their category, but for which no on-site inspections have been carried out since 2019. Supervision is also limited for insurance intermediaries (no on-site inspections since 2021, despite concerning findings during the last inspections) and lenders (10 on-site inspections in six years and 8 remote inspections, all carried out in 2019), despite the existence of specific risks. Priority is given to consumer credit lenders, which are considered the highest risk, while mortgage and social lenders remain largely overlooked. However, the latter also have vulnerabilities that call for an assessment of the effective implementation of mitigating measures – an assessment that cannot be carried out through the FSMA's off-site inspections.

Table 3.2. FSMA inspections (2019-2024)

	2019	2020	2021	2022	2023	2024	Total
On-site inspections							
Lenders	5	0	4	0	0	1	**10**
Insurance intermediaries	88	0	36	0	0	0	**124**
Small alternative OPCA	3	0	0	0	0	0	**3**
Off-site inspections							
Lenders	8	0	0	0	0	0	**8**
Insurance intermediaries	98	240*	0	0	40	22	**400**
Small alternative OPCA	0	0	20	0	0	57*	**77**

Note: * These inspections were carried out on an ad hoc basis, for information purposes only, to gain a better understanding of how the sector operates. No findings or orders were issued following these inspections. For follow-up, refer to table 3.4 in section 3.6.
Source: FSMA

377. The nine VASPs issued with provisional authorisation were subject to on-site inspections, for those assessed as higher risk (two VASPs), or off-site inspections (seven VASPs) (see below for the results of these inspections).

SPF Finance – Treasury

378. The 2015 MER recommended that Bpost implement AML/CFT supervision. SPF Finance has been supervising Bpost since 2016. The last inspection was carried out in 2020 and was followed by an action plan that was completed in 2023. Given the ML/TF risks posed by the financial services offered by Bpost, particularly in relation to the predominant use of cash and the relative anonymity of Bpaid cards, the frequency of inspections would appear to be insufficient.

3.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on FI and VASP compliance

BNB

379. BNB plays a key role in raising awareness among FIs, in particular through its regularly updated website, which is commended by the private sector and contributes to a better understanding of AML/CFT obligations. BNB is recognised for its availability and interaction with FIs. Raising awareness among FIs also relies heavily on professional associations (Febelfin, Assuralia, PayBelgium), whose work is essential but needs to be supplemented by more direct communication from the BNB to FIs. The lack of regular dialogue with FIs (e.g. AMLCO of large banks, payment institutions and electronic money institutions) and professional associations limits the direct reporting of their issues, which slows down the adjustment of supervisory priorities and hinders a more optimal mutual understanding and more appropriate supervision.

380. The *AML platform* was launched in 2021 and promotes public-private cooperation by bringing together the BNB, the FSMA, SPF Finance/Treasury, the CTIF, SPF Justice, the police and professional associations. Although it has been holding regular meetings since June 2021, it remains little known among FIs, and its concrete impact on FIs' understanding of risks remains limited in the absence of accessible publications or conferences.

381. The BNB communicates regularly with FIs through thematic circulars, which serve as guidelines and reflect the analysis of sectoral practices (e.g. de-risking, repatriation of assets, fund transfers). This approach helps to clarify regulatory expectations and harmonise practices, thereby strengthening FI compliance. Nevertheless, FIs still express a need for guidance in other areas that they consider to be insufficiently explored by the BNB at present (e.g. management of basic banking services). There is also a need for more operational guidance.

382. Finally, the training efforts organised by the BNB remain limited: only two AMLCO meetings have been held since 2019. However, the BNB regularly participates in seminars and training courses organised by in-service training providers.

FSMA

383. The FSMA organises several outreach initiatives, including an AMLCO Day, focusing on topics identified during supervision (see example in box below) and feedback from the CTIF. For example, the issue of suspicious transaction reports (their importance and the quality of the information provided) was the subject of a specific presentation during the first AMLCO Day. The FSMA also publishes newsletters dedicated to AML/CFT, which are well known and consulted by FIs, but whose frequency remains limited in view of the needs of the sector. The FSMA also organises regular meetings with professional associations. It also participates in conferences organised by private operators in particular.

Box 3.2. Example of an inspection followed by outreach actions

Facts: In December 2022, an on-site inspection of an OPCA and OPCVM management company revealed shortcomings in the understanding of the concept of "customer". A remediation plan was implemented to address these shortcomings.

Actions taken: The FSMA subsequently conducted a survey in 2023 among the AMLCOs of a number of OPCVM management companies. The aim of the survey was to identify the difficulties encountered in practice. It revealed that the interpretation of the concept of "customer" was a widespread problem in the sector.

Outcome: Given the scale of the issue, the FSMA included this topic on the agenda of its AMLCO Day 2023 in order to clarify the concept of customer for the entire sector, not just for the entity initially inspected.

384. The FSMA supervises FIs with very diverse profiles in terms of size, risks and business models. However, its outreach actions often remain general in nature, which limits their relevance for certain players with specific business models, such as alternative OPCA/OPCVM management companies, which are not always covered by content that is tailored to insurance intermediaries or bureaux de change, which have a more direct relationship with customers.

385. Some FIs, such as insurance intermediaries, receive sector-specific support through professional associations. In particular, a sectoral code relating to the distribution of financial products has been developed with Assuralia.

386. Supervision feedback was published after certain inspections, notably in January 2025 for the currency exchange sector, and in 2020 for insurance intermediaries, bank brokers and lenders. However, the frequency of this feedback remains irregular. Short outreach films produced in 2021 were well received.

387. With regard to VASPs, the FSMA has created a section on its website dedicated to VASPs, which contains answers to frequently asked questions, useful for this sector, which is unfamiliar with AML/CFT requirements. It has expanded this information based on its review of registration applications submitted during the transitional period (see above). For example, it has clarified the FSMA's expectations regarding the measures to be taken by VASPs when AML/CFT obligations are fulfilled by third parties, such as Fintech or RegTech companies.

SPF Finance – Treasury

388. Guidelines have been developed, but the evaluation team was unable to evaluate them.

3.6.1. Impact of controls, administrative measures and sanctions

BNB

389. FIs under BNB supervision generally implement remedial measures in a spirit of cooperation and compliance. Follow-up is mainly carried out through regular meetings and the submission of documents, with re-inspections being less frequent. However, remediation times are often long (see box), as the BNB favours an educational and graduated approach, using orders without penalties, which are sometimes extended formally or de facto.

Table 3.3. Examples of remediation pathways for CIs under BNB supervision

	Credit institution A) [one of the four main Belgian CIs]	Credit institution B)
Inspection	10 months (between March and November 2021)	1 year (October 2019 to October 2020)
Shortcomings identified	Score 3 out of 4 (significant - serious breaches)	Score 3 out of 4 (significant - serious breaches), including critical breaches in correspondent banking and vigilance with regard to non-resident customers.
Remediation time	The report was published in May 2022, but the implementation monitoring was not completed until April 2024 (23 months later), which is considered a long time to ensure effective remediation.	The action plan was adopted late, in January 2021, followed by an enhanced inspection that was only completed in February 2023 (over two years later), illustrating the prolonged implementation of corrective measures.
Follow-up	The time between identifying the shortcomings and validating the corrective measures was also considered excessive.	Work still in progress: internal audit requested for inspection, indicating that corrective measures remain to be finalised.

Source: BNB

390. More severe administrative measures (e.g. temporary suspension of activity), although proven to be effective, are used only sparingly.

391. The BNB rarely publishes its administrative measures and, when it does, it does so anonymously, limiting their deterrent effect. One case illustrates this trend, where an FI obtained a waiver of publication of its name following the exercise of its right to be heard prior to the adoption of the measure by the BNB.

392. The BNB favours "indirect deterrence" (hearsay, press), which is considered insufficient. In several cases, the shortcomings identified called for measures more proportionate to the seriousness of the facts (such as, for example, two successive inspections resulting in the most severe score of 4/4; lack of screening of SFC lists when entering into a business relationship).

Box 3.3. Credit institution c)

This case illustrates the legal constraints and excessive caution limiting the use of sanctions by the BNB.

In the same case, that of CI c), the BNB considered disciplinary action three times before deciding not to proceed on each occasion:

2020: referral of the case to the Public Prosecutor's Office, where the investigation is still ongoing. This referral was accompanied by a decision to wait for the outcome of the criminal proceedings before considering the application of sanctions, so as not to interfere with them.

2021: CI c) terminated 468 business relationships without complying with its due diligence obligations, despite the measures imposed by the BNB in 2020 and a significant risk of transactions not being reported to the CTIF. The sanction was dropped due to the ambiguous wording of the original measure.

2023: Despite late remediation, the BNB considered that failure to meet a remediation deadline did not in itself justify a sanction.

393. Several factors hinder the implementation and effectiveness of the overall process leading to the application of administrative sanctions: the complexity of the sanctioning procedure[116], the lack of

[116] Summary of the process leading to the application of a sanction by the BNB sanctions committee: After an initial decision on the appropriateness of taking action, the AML/CFT Group submits a written report to an assessment committee. If the committee decides to proceed, the AML/CFT Group drafts a referral to the auditor and compiles a file of evidence, which is submitted to the BNB management committee. The auditor, who manages all matters

dedicated resources (particularly legal and auditing resources), excessive caution, fear of appeals and the requirement for the AML/CFT Group to demonstrate the underlying causes of the breaches in order to justify disciplinary action. This results in paralysis of the BNB's action, thus depriving it of the use of a fundamental part of its powers. When sanction procedures are initiated, the length of the overall sanctioning process (several years, sometimes at the auditor stage alone) reduces its deterrent effect and may even influence the amount of the fine. As a result, the number of fines issued by the BNB is extremely low (only one in ten years).

394. The lack of resources dedicated to legal advice and guidance significantly hinders the effectiveness of the system. Since 2016, the number of FTEs allocated to these functions has remained virtually unchanged, and is considered to be clearly insufficient: 0.5 FTE for legal advice (0.3 in 2016) and 1.5 FTE for administrative sanctions (1.35 in 2016). The sanctioning process is long and complex (see previous paragraph). Due in particular to the limited resources allocated to the auditor, this mechanism remains unproductive, with an average of 1.2 cases handled per year, a rate considered highly insufficient to ensure that sanctions have a dissuasive and responsive effect, being intended to address the most serious failures. At present, only a few cases are under investigation, despite some having been referred some time ago (see table below), which reflects in particular the complexity of the cases and the lack of human resources, and contributes to the slowness of the process.

Box 3.4. Examples of the time taken for the supervisory process and follow-up

These cases illustrate the slowness and shortcomings in the handling of serious infringements (score 4/4) by the NBB, particularly the late referral to the auditor and the fact that remedial action takes several years.

Excessive delays between inspection and referral to the auditor:

- FI 1: Belgian CI. Inspection at the end of 2020-beginning of 2021, referral not until March 2022 (+1 year), investigation still in progress
- FI 2: Belgian CI. Inspection between July 2020 and March 2021; December 2022: notification to the FI of the serious nature of these shortcomings; auditor not notified until the end of July 2023 (+18 months after notification of the shortcomings), investigation still in progress.
- FI 3: Inspection in 2021, referral in September 2022 (+1 year), investigation still in progress.

Very long action and remediation plans:

- FI4: One of the four main Belgian CIs. Inspection between November 2021 and October 2022, score 4/4, auditor appointed in July 2023, investigation still in progress and compliance is also still being checked as of 14 February 2025 (end of on-site visit).
- FI5: Inspection from Q3 2021 to Q2 2022, referral in June 2023 (+1 year), investigation still in progress, remediation not completed until summer 2024.

395. Another negative effect of this lack of regular sanction procedures is the lack of case law, depriving the BNB and the private sector of a stable frame of reference for interpreting and applying the regulations. In comparison, frequent and clear decisions by a sanctions committee would clarify the practical application of the regulatory framework and provide better guidance for FI practices.

FSMA

audited by the BNB, examines the evidence for and against. The auditor then submits their conclusions to the management committee, which decides whether to continue the sanction procedure and whether to refer the matter to the sanctions committee or propose a settlement.

396. As explained in section 3.5, some of the FSMA's off-site inspections are primarily informative in nature (improving the FSMA's understanding of a sector or entity). These inspections have limited effectiveness in terms of FI compliance, as they do not include verification of the AML/CFT system or any remediation orders. By contrast, off-site compliance inspections result in corrective measures, although these remain formal (e.g. updating policies and procedures) (see box below), as these off-site inspections are designed to check the formal compliance of FIs. Verification of follow-up mainly concerns the analysis of documents provided by the FI, while on-site visits, which are the most effective means of ensuring effective and thorough remediation, are rarely used.

Table 3.4. Results of thematic or ad hoc and off-site inspections by the FSMA

Thematic or ad hoc inspections not resulting in remedial orders:
2020: 240 insurance intermediaries ("ad hoc" inspections) →no orders.
2021: 20 small alternative OPCAs (thematic inspection) →no orders.
2022: 31 branches of alternative OPCAs (thematic inspection) → no orders.
Off-site inspections (compliance checks) resulting in corrective measures:
2019: 98 insurance intermediaries inspected → 251 offences detected.
2023: 40 insurance intermediaries inspected → 61 offences detected.

397. Delays in remediation are not usually sanctioned immediately, as the FSMA favours support and additional time is often granted. However, a clear refusal to comply leads to more severe measures.

398. The FSMA has an administrative sanction procedure, which can also lead to a settlement agreement. This procedure is rarely used in AML/CFT matters. In 10 years, only two administrative sanctions relating to AML/CFT have been applied by the FSMA's sanctions committee. Several factors may explain this shortcoming: insufficient (or incomplete) understanding of the role of administrative sanctions: the usefulness of their punitive function in the most serious cases, either alone or in addition to an administrative measure; their deterrent effect, both for the institution concerned and for the sector as a whole; and their educational value, as the reasoned decisions of the sanctions committee contribute to the development of a body of case law. In addition, as in the case of the BNB, there is a fear of appeals and the slowness of the process, which involves, in particular, referral to an auditor to investigate the cases. This shortcoming is partly offset by the occasional use of serious administrative measures, such as temporary suspension of activity or deregistration, the financial consequences of which act as a dissuasive. For example, one bureau de change was suspended following an inspection carried out by the FSMA between late 2024 and early 2025. After a one-month suspension, the bureau de change confirmed to the FSMA in April 2025 that it had taken the expected measures. These measures are published by name on the *"Actualités et mises en garde"*(news and warnings) web page and on the public record of the FI concerned, increasing their visibility. Creation of a web page dedicated to publishing serious administrative measures by name and increased use of sanctions are desirable.

399. Supervisory measures are largely perceived as a tool for outreach and guidance. They focus mainly on the formal compliance of FIs, with findings regularly resulting in orders being sent to non-compliant FIs. These actions have a positive effect, particularly on the compliance of currency exchange offices and, to a lesser extent, insurance intermediaries. Nevertheless, they still appear insufficient to ensure the adequate and effective implementation of mitigating measures by FIs.

SPF Finance – Treasury

400. Bpost has met the deadlines for remedying the shortcomings identified during supervision in 2020. Quarterly meetings enable Bpost to continue improving its compliance over time.

4 Non-financial sector supervision and preventive measures

The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this chapter are R.22, 23, 28, 34 and 35 and elements of R.1, 29 and 40.[117]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) All DNFBPs are subject to procedures for access to the profession. These systematically include criminal record checks, identity and management information checks, and only in some cases, education requirements (diamond dealers, accountants and lawyers) and verification of beneficial ownership. However, these controls are not always carried out systematically after entry into the profession.

b) Supervisory authorities for diamond dealers, casinos and accountants have a very good understanding of ML risks. Supervisors for estate agents, company service providers/business centres[118] and statutory auditors show a good understanding. Understanding is more limited among other self-regulatory bodies (SRBs), whose knowledge of vulnerabilities is similar to that of the reporting entities themselves. Understanding of TF risks is generally low across all authorities. Furthermore, sectoral risk assessments (SRAs) lack granularity and, for the most part, merely repeat the conclusions of the national risk assessment (NRA), with the exception of the SRA conducted by the SRB for accountants (ITAA).

c) The majority of DNFBPs have a very limited understanding of ML/TF risks. Accountants demonstrate more in-depth knowledge and statutory auditors demonstrate sufficient knowledge of the risks specific to their sectors of activity. On the other hand, real estate agents, diamond dealers and business centres show significant shortcomings, mainly due to the absence of internal risk assessments and/or regular updates of their analyses. This weakness has a direct impact on their ability to detect and report suspicious transactions.

[117] Rec. 1, 22, 23, 28, 29, 34 and 40 are under review, see the Technical Compliance Annex.

[118] In the category of service providers to companies, only domiciliation services or business centres (i.e. the provision of a head office) are subject to the AML/CFT regime (see the TC Annex, R.22).

d) The lack of supervision is one of the main weaknesses of the system, particularly in sectors most exposed to ML/TF risks. SPF Economy, which is responsible for several high-risk sectors (diamonds, business centres, real estate agents), faces a critical shortage of human resources: with only 16 FTEs, it can only carry out a very limited number of controls. As a result, these sectors remain largely unsupervised and monitoring is almost non-existent, despite high rates of non-compliance.

e) For self-regulated professions, inspections are more frequent. However, with the exception of the ITAA, the depth of this work remains rather limited, particularly in the area of AML/CFT. As regards notaries, inspections are not fully grounded in a risk-based approach - all notaries are inspected every three years and the sampling of files focuses on risk areas, namely real estate and companies.

f) The Belgian Gaming Commission (CJH) does not have the necessary autonomy to hire its own staff and has only five employees to monitor 7,000 gaming venues. This structural shortcoming limits its ability to carry out effective AML/CFT supervision in casinos, which are inherently exposed to a high ML risk.

g) The reporting activity of the DNFBPs varies greatly between sectors and remains particularly low among diamond dealers, lawyers and business centres. In these three sectors, the reports (STRs) transmitted are often of little relevance. The transmission of STRs from lawyers via the presidents of the bar association raises questions, particularly regarding transmission timelines and the information provided to the lawyers making the declarations.

h) Although administrative sanctions are sometimes applied, they remain too rare and anonymous, which reduces their dissuasive impact. Among notaries and lawyers, guidance is largely preferred over sanctions, which weakens the deterrent effect, while still having a positive impact in terms of raising awareness. For business centres, despite a high rate of non-compliance and a significant number of warnings and reports, administrative fines are few and far between. On the other hand, for diamond dealers, SPF Economy does not have administrative sanctions for minor breaches, which sometimes leads to licence suspensions, which appears disproportionate.

i) The limited number of inspections makes it difficult to fully measure the impact of the measures on the compliance rate of the sectors most at-risk beyond the impact on the penalised entity. However, the training and awareness-raising activities organised by the supervisory authorities and the tools made available to reporting entities have contributed to a certain awareness of AML/CFT obligations among reporting entities, although they have so far been limited in scope to date.

Key Recommended Actions (KRAs)

Belgium should:

a) Introduce more frequent inspections in the highest-risk sectors (diamond dealers, estate agents and business centres) by increasing the number of on-site inspections and ensuring regular monitoring; as well as by systematically standardising preparations for inspections in order to allocate the appropriate resources to each supervisory activity based on risks.

b) Strengthen the sanctions regime in all DNFBP sectors to ensure a proportionate and dissuasive response, particularly to serious breaches, including by applying the full range of sanctions available, and by publishing decisions by name to reinforce their dissuasive effect.

c) Strengthen the capacity of SPF Economy in the area of AML/CFT and ensure that AML/CFT issues are fully integrated into all its activities, in order to optimise awareness among the entities under its responsibility.

Other Recommended Actions

Belgium should:

a) *Diamond dealers* – Introduce a graduated administrative sanctions regime to deal with minor licence infringements (without systematically resorting to heavy measures such as suspension); improve the impact of awareness-raising actions, including the information disseminated by the Antwerp World Diamond Centre (AWCD), by integrating mechanisms to verify understanding.

b) *Business centres*[119] – Strengthen the sector's understanding of AML/CFT obligations and ensure that inspections are carried out regularly.

c) *Notaries* – Review the procedures for appointing notaries responsible for inspections in small provinces to guarantee the necessary neutrality.

d) *Lawyers* – Clarify the expectations and obligations of bar association presidents regarding the dissemination of STRs filed by lawyers, in terms of deadline and information to lawyers making the declarations.

e) *Casinos* – Allocate the necessary human resources to the Belgian Gaming Commission for effective monitoring of the establishments under its control.

f) Increase the depth of AML/CFT supervision while ensuring that it is truly risk-based, for all DNFBPs, prioritising those most at risk.

g) Improve the exchange of information between the judicial authorities and the DNFBP supervisory authorities to enable the rapid transmission of convictions so that supervisory authorities can take the necessary disciplinary measures without delay, and so that authorities can further profile of DNFBPs at risk, in order to better focus supervisory efforts on high-risk DNFBPs.

h) Strengthen practical training focused on key obligations (customer verification, BO identification, transaction analysis) and on sector-specific ML/TF risks, including targeted and regular training programmes for high-risk sectors (diamond dealers, real estate agents, business centres and notaries), as well as for certain medium-risk sectors (lawyers).

i) Distribute risk analyses (NRA and SRA) to all DNFBPs.

[119] See also RD h) in IO 1

Overall Conclusions on IO.4

A remaining deficiency in the measures applicable to company service providers leaves a considerable gap in regulated activities, given the high level of risk assigned in Belgium to potential abuses by legal persons to which these providers are associated (IO 1 and 5). Particular importance is also attached to persistent gaps in the effective implementation of AML/CFT measures, particularly in the most at-risk sectors – diamond dealers, business centres and real estate agents.

Although the authorities have an overall understanding of the risks, this knowledge is not sufficiently translated into rigorous supervision that is proportionate to the vulnerabilities of the sectors. Diamond dealers, real estate agents and business centres, the materiality of which is very important in the Belgian context, thus present concerning levels of compliance, with insufficient risk analyses, limited application of due diligence obligations and insufficient use of enhanced monitoring measures.

Inspections are conducted across all sectors, but the authorities' risk-based approach remains incomplete, including for the most at-risk sectors. In addition, the resources allocated to supervision are insufficient, particularly for diamond dealers, to ensure effective monitoring and target the entities most exposed to ML/TF. While conducted inspections reveal systemic shortcomings, the low number of such controls and the lack of follow-up restrict their remedial effect. This is particularly the case for business centres.

Authorities do have some remedial measures and sanctions at their disposal, but often favour an educational approach that focuses on accompaniment rather than sanctions. Sanctions applied lack any real dissuasive effect, as they are infrequent, often anonymous and not accompanied by structured monitoring of sanctioned entities.

Although increasing, awareness-raising and training efforts remain too general and not sufficiently tailored to the operational realities of the reporting entities, which hinders effective better ownership of the AML/CFT obligations.

Major improvements are required.

Belgium is rated as having a Moderate level of effectiveness for IO.4.

Immediate Outcome 4

401. The evaluation team applied the following weighting to assess the implementation of preventive measures by DNFBPs: extremely important for diamond dealers; very important for company service providers (business centres), estate agents, chartered accountants, notaries and casinos; moderately important for lawyers and auditors; and less important for other DNFBPs. The details of the weighting of each sector are to be found in the introduction.

402. With regard to company service providers, as indicated under IO 1, the 2017 AML Law includes within its scope only one of the five categories of activities identified by the FATF – providers of registered offices for companies (business centres) – without justification on the basis of risk.

4.1. Licensing, registration and controls for DNFBPs preventing criminals and associates from entering the market

403. Several authorities – public authorities or self-regulatory bodies (SRBs) – share responsibility for market entry supervision (see the Introduction).

404. Diamond dealers - Since the last assessment, the conditions for registering diamond dealers have been strengthened, particularly in terms of integrity, training and expertise. Between 2019 and 2024, the number of diamond dealers fell (by 163 out of a total of 1,390 licensed businesses), with only 48 new licences issued over the period (see the Introduction). These figures suggest a tightening of market entry conditions.

Table 4.1. Diamond dealers: licensing, refusals, suspensions and terminations

Year	New licences	Applications rejected	Licences suspended	Deregistered
2020	68	1	/	139
2021	84	1	1	143
2022	85	0	0	74
2023	74	3	1	82
2024	48	1	0	72

405. Diamond dealers must obtain a licence from SPF Economy before operating, with strict requirements including administrative documents, criminal record statements, information on directors, and a seminar including AML/CFT training. SPF Economy carries out rigorous checks on the information provided, using the ORBIS[120] database in particular to verify beneficial owners (BO) and politically exposed persons (PEP) among directors and shareholders. Additional research is carried out on the internet and social media to map companies and identify any anomalies.

406. The number of deregistrations remains significant, although it is falling. SPF Economy refuses few licensing applications, mainly when the files are incomplete or in cases of doubt about the company. However, SPF Economy does not have administrative penalties for licences, which limits its ability to punish irregularities without resorting to extreme measures. In the event of irregularities, the only option is licence suspension, whereas a graduated financial penalty would allow for a more proportionate and dissuasive response.

407. *Business centres* - Since 2018, these company service providers have been required to register with SPF Economy, which they can do online. The verification process covers directors and their BOs and criminal records. However, there is no automated supervision of changes of directors and registered offices once registration has been completed. This situation may allow high-risk individuals to discreetly join the management of business centres after registration, without triggering further checks, even though entities are legally required to inform SPF Economy of such changes. The below highlights a marked trend towards the approval of applications, with 340 registrations in the last five years, 65 applications refused and 30 classified without further action[121], and a few rare cases of voluntary withdrawals. With an average of 13 refusals per year, the rejection rate is reasonable.

[120] Orbis is an analysis tool and global database developed by a private firm.

[121] Applications classified "without further action" correspond to files for which the information necessary for their evaluation has not been provided. Despite a request for additional information, no response was received, which led to this status being assigned.

Table 4.2. Business centres: status of applications for registration (2020-2024)

Year	Applications approved	Applications rejected	Applications withdrawn	Without further action
2020	71	16	2	5
2021	58	14	5	8
2022	104	18	1	8
2023	79	13	0	7
2024 (end of Nov.)	50	6	5	4
Total	283	67	13	32

Source: SPF Economy

408. Post-registration checks in this sector reveal a persistent risk of non-compliant operators on the market, requiring stricter follow-up from the registration phase onwards. An investigation by SPF Economy in 2022 revealed a high rate of operators operating without registration (89 out of 147), which constitutes a significant ML/TF risk. However, SPF Economy takes this issue seriously. It sanctioned these infringements with warnings and fines, prompting 65 operators to comply with the rules, and carried out 320 checks for non-registration between 2021 and 2023, resulting in 121 reports, 24 warnings and sanctions totalling EUR 148,750. The lack of systematic monitoring of changes in directors and registered offices compromises the authorities' ability to detect and prevent the infiltration of criminal structures post-registration. Given the sector's high exposure to ML/TF risk and the high rate of non-compliance, further checks should be carried out in the short term, followed by dissuasive sanctions where necessary.

409. *Real estate agents* - The Professional Institute of Real Estate Agents (IPI) carries out targeted checks and has effective tools to detect unregistered real estate agents. The quality of its measures to control access to the profession and entry to the market is very good. In 2023, the IPI carried out 555 checks and inspections to ensure that real estate agents were registered and compliant with regulations, which led to 16 convictions for non-compliance with the rules in force. This level of monitoring demonstrates a significant effort to strengthen the integrity of the real estate agent sector and limit the infiltration of fraudulent operators. The IPI also carried out targeted audits of all companies in 2024 to ensure that all agents operating in these companies were properly registered and in compliance with the regulations.

410. *Legal and accountancy professionals*[122] - Subject to strict measures to gain access to their profession. These include rigorous training and skill requirements, as well as, in most cases, criminal record and integrity checks. These professionals are also subject to numerous ethical rules, compliance with which is regularly monitored. The misuse or fraudulent use of professional titles is a criminal offence and is prosecuted as such when detected, most often following reports from third parties. The SRBs responsible for these professions do not have investigative powers and therefore respond reactively to cases of illegal professional practice.

411. Access to the profession of *notary*, which is subject to a decision by the public authorities, is strictly regulated by law, with rigorous requirements in terms of qualifications, training and aptitude, as well as criminal record and integrity checks. Two authorities are responsible for detecting and dealing with non-compliance with obligations: the management committee of the National Chamber of Notaries and the provincial chambers of notaries (see the Introduction). Similarly, the Belgian Bars have robust procedures for admission to the profession of lawyer, ensuring rigorous screening of candidates. Any change in the statutes of a law firm must be submitted to the president of the bar for prior approval. Operation by criminal entities is limited, as only lawyers can manage and control a law firm.

412. For *chartered accountants*, the Institute for Tax Advisors and Accountants (ITAA) keeps a register of chartered accountants authorised to practise. Although licensing procedures are in place (including

[122] Among these professions, the categories most relevant for materiality in Belgium include notaries, chartered accountants and auditors.

rigorous educational, training and aptitude requirements, and criminal record checks on applicants and ethical rules), refusals of applications remain rare, largely due to the strict procedures. All chartered accountants are required to keep their professional information up to date, and the ITAA actively monitors the compliance of its members. The ITAA does not carry out checks on the shareholding structure of accounting firms, which could facilitate criminal infiltration through opaque legal structures, in accordance with the scope of its legal obligations.[123] However, during quality reviews of its members, the ITAA verifies that firms still meet the legal requirements for the profession of chartered accountant,[124] in particular that the majority of the voting rights of the firm are still held by ITAA members, which mitigates the risks.

413. *For statutory auditors*, access to the profession is strictly regulated, requiring a criminal record check, extensive training and numerous exams in addition to a Master's degree and a three-year internship supervised by an auditor, followed by an aptitude test. As a result of these stringent criteria, refusals are rare and mainly concern foreign candidates whose qualifications are not considered equivalent to Belgian standards. Post-registration follow-up is limited.

414. *Casinos* - When it receives a licence application or request for renewal, the Belgian Gaming Commission (CJH) conducts a thorough check on the transparency of the institution's ownership and management, its financial stability as certified by an accountant, and carries out criminal record checks on directors and shareholders holding at least 20% of the shares. It also investigates the BOs of gaming operators by examining the group's organisational chart and using various means, including external advice from specialist lawyers in the event of difficulties. The CJH closely monitors the entry of casinos into the market and actively blocks illegal gaming sites. In particular, the CJH carries out systematic searches leading to geo-blocking and systematically issues penalties. It also publishes a blacklist of illegal sites to inform and protect players. Since the last FATF evaluation, it has blocked 784 illegal sites. However, its post-approval follow-up is largely inadequate.

4.2. Actions by the supervisory authorities to identify, understand and promote understanding of TF risks by DNFBPs

415. The effectiveness of the Belgian authorities in identifying and understanding ML/TF risks varies according to the sectors of the DNFBP. While the supervisory authorities for diamond dealers and casinos have a good understanding of ML risks, this understanding is more limited in other sectors, particularly among SRBs. The risks of TF remain poorly understood overall, and awareness-raising efforts remain insufficient, which weakens their ability to detect and prevent offences (see section 4.3).

416. SPF Economy has a very good understanding of ML/TF risks related to diamond dealers, thanks to the use of data from licences, annual reports and strict controls on shipments and imports. However, the lack of AML/CFT resources within SPF Economy (see section4.3) limits the dissemination of this understanding to reporting entities. Outreach initiatives are insufficient. Furthermore, national and sectoral risk analyses do not yet appear to have had any significant impact on the sector.

417. SPF Economy has a good basic understanding of the risks in the *real estate agent* sector. Risk analysis is mainly based on information from the sector, including the general survey[125] conducted in 2021 (see below) and data from the police, the CTIF, the Chamber of Notaries and open sources. It is supplemented by information on consumer protection.

[123] Article 8 of the Royal Decree of 11 September 2020 laying down the details of the public register of accountants.

[124] Article 10 of the law of 17 May 2019.

[125] A general survey is a control measure used by SPF Economy that involves collecting and analysing information on the implementation of obligations from all entities subject to them in a given sector, see section 4.5

418. The authorities are aware of certain specific risks, in particular the overvaluation and undervaluation of property. They also understand the ML risks arising from large-scale real estate transactions that escape the traditional intermediation channels, in particular acquisitions made through integrated real estate companies, where the final purchaser does not use a notary, estate agent or Belgian financial institution. However, real estate agencies operating internationally and certain specialised services, such as B2B, are less well understood as they are not widely monitored. This situation is mainly due to a lack of staff dedicated to AML/CFT supervision. SPF Economy and the IPI promote AML/CFT obligations to a certain extent, but these efforts remain limited. Although the 2023 ML NAR has been distributed to real estate agents, understanding of the risks in the sector remains variable. The IPI has also developed a detailed manual and an IT risk analysis tool (ORIS), but these resources appear to be little used.

419. Since the sector became subject to AML/CFT requirements in 2018, SPF Economy has increased its understanding of the ML/TF risks of *business centres*. This assessment is based on several sources, including a sector survey conducted in 2022, and government data (in particular with police services as part of the BELFI project[126]– see IO.9). The analysis takes into account key factors such as turnover, number of domiciled customers, bankruptcies, dissolutions and address changes. The authorities estimate that around 40% of registered business centres present a significant or high risk. They also recognise the significant ML risks associated with illegal service providers, particularly due to their potential role in providing addresses to inactive or shell companies. Given the lack of human resources dedicated to AML/CFT, SPF Economy is forced to prioritise the identification of illegal operators (those not registered) at the expense of outreach to registered service providers. As a result, efforts to promote a better understanding of the risks in the sector remain in their infancy.

420. SRBs in the *legal and accounting professions* generally have a limited and fragmented understanding of ML/TF risks, based mainly on the NRA and ad hoc observations. Only the ITAA has a structured framework, with over ten years of analysis based on a variety of sources, including AML investigations and quality controls. Using these tools, the ITAA identifies between 250 and 300 high-risk members (chartered accountants) and provides a risk standard for its reporting entities.

421. The National Chamber of *Notaries* strengthened its understanding of ML/TF risks in 2021 by commissioning an academic to carry out an SRA. This study highlighted underestimated vulnerabilities, particularly those related to the creation of companies, and enabled the notarial authorities to better understand the extent of the risks to which the profession is exposed. However, this analysis has not been updated or integrated into a sector-specific methodology to monitor risks on an ongoing basis. The Chamber nevertheless takes into account CTIF publications to improve its understanding of the risks. While the National Chamber of Notaries is engaged in outreach efforts through the 2021 SRA and certain training activities, regulated entities have expressed a growing need for regular updates to better monitor developments in ML/TF risks.

422. For *lawyers*, the bars have a limited and outdated view of ML/TF risks, identifying certain risks related to quality accounts and considering that large firms are less exposed than small firms, thanks to stricter internal procedures. However, their approach does not follow a systematic analysis methodology and is based more on ad hoc findings than on a genuine analysis of vulnerabilities. In addition, the bars have not yet incorporated the 2023 NRA into their risk assessments, as they only received it at the end of 2024. Their analytical framework is therefore still based on the 2019 NRA, which limits their ability to identify recent developments in ML/TF patterns. The lack of a structured framework for monitoring and analysing trends makes it difficult to accurately assess how risks evolve over time and therefore constitutes a significant weakness in the ML/TF risk management for this profession.

[126] The BELFI project is a project to combat fraud through enhanced cooperation between judicial, tax and administrative authorities (see box under IO.10).

423. The CJH has a very good understanding of ML/TF risks in the casino and other gambling sector, thanks to a sectoral analysis completed in September 2024, although this had not yet been published at the time of the visit. Its approach is based on a detailed analysis of the risks associated with different products, customer types and the interactions between them. Strict mitigating measures are in place, including a ban on current accounts for players, control of chips and transactions, and enhanced monitoring of high-risk profiles (such as PEPs whose identity cannot be verified).

424. The CJH maintains ongoing risk assessment, with formal discussions with operators twice a year and operational discussions three to four times a year. It also plays an active role in outreach to reporting entities, organising eight training sessions (four per official language) in 2024 for 1,100 people. The guidance (White Paper) – currently being developed – is not yet available to gaming operators, who have expressed a growing need for clear guidelines, suggesting that support could be improved.

425. Finally, the Audit Oversight Board (BAOB) has an adequate understanding of the risks associated with *auditors*, which is proportionate to the (limited) ML risk to which the sector is exposed. The BAOB conducts annual surveys on ML among auditors and prepares annual individual risk assessments, and conducted a sectoral risk analysis in 2022. Statutory auditors receive annual information on risks and typologies from the BAOB. The BAOB has also published a tool on its website to help auditors carry out risk assessments. Auditors also have access to a manual published by the professional organisation, the Institute of Statutory Auditors (IRE).

4.3. Understanding of existing and emerging ML/TF risks by DNFBPs

426. The limited understanding of ML/TF risks by DNFBPs, including those considered high risk, is a major obstacle to the effectiveness of the AML/CFT system. Most do not conduct a comprehensive risk assessment within their organisations. In the absence of such assessments, these entities do not fully understand their own exposure to ML/TF threats (which they perceive as low) and, as a result, do not adopt appropriate due diligence measures. This significantly reduces their ability to detect and report suspicious transactions, thereby weakening the effectiveness of due diligence measures.

427. The fact that the majority of DNFBPs consider their sector to be low risk, despite the vulnerabilities identified by the authorities, reflects a discrepancy between the risk perceived by the reporting entities and the reality of the ML/TF methods and typologies observed. This lack of awareness compromises the effective implementation of due diligence obligations, particularly with regard to suspicious transaction reporting and training for relevant staff.

428. The conclusions and results of national ML/TF risk analyses have not been assimilated or integrated by the majority of DNFBPs. Although some have had access to a recent SRA, these analyses usually simply repeat the conclusions of the NRA, without providing an in-depth and contextualised assessment of the specific vulnerabilities of each sector. This partial or insufficient dissemination of risk analyses limits the ability of reporting entities to improve their compliance and develop internal assessments of their own risks.

429. *Diamond dealers'* understanding of ML/TF risks is very limited, despite their high exposure to such risks. While some are aware of their AML/CFT obligations, risk assessment within companies remains inadequate, and awareness of ML risk is virtually non-existent. Diamond dealers generally limit themselves to an initial customer assessment when establishing a relationship, but this is rarely reviewed over time, as diamond dealers consider themselves to be "well acquainted" with their customers. They do not carry out an overall analysis of their company's ML/TF risks. This static approach considerably limits their ability to detect possible changes in customer behaviour or unusual transactions.

430. The supervision carried out by SPF Economy between 2020 and 2023 confirms major shortcomings in the implementation of AML/CFT obligations (see next section). Of the 17 entities supervised, 12 were found to have shortcomings in relation to the absence of risk assessment. Although an *AML Policy* was drawn up in 2020 and updated regularly (most recently in June 2024) by the professional organisation Antwerp World Diamonds Center (AWDC) in collaboration with SPF Economy to help identify risks, its adoption by the entities subject to the obligations remains limited, despite outreach efforts aimed at professionals. Furthermore, shortcomings in the AWDC's understanding of the risks give cause for concern.

431. *Real estate agents* also have very limited understanding of the risks, particularly those operating in the residential real estate sector. These professionals have fragmented knowledge of the risks and struggle to articulate them accurately. They tend to underestimate their exposure, considering that their business mainly involves local customers and few suspicious transactions. This misperception reduces the effectiveness of AML/CFT obligations and weakens the detection of ML schemes in real estate. Furthermore, the ML NRA and the ORIS tool (see above) are largely unknown or are not used by real estate agents, which limits their integration into industry practices.

432. When real estate agents carry out a risk assessment, it is limited to a summary analysis of the customer. A survey conducted by SPF Economy in 2021 highlighted significant shortcomings in risk identification for 42% of the real estate agents inspected. SPF Economy has not clearly defined the profile of high-risk real estate agents who should be subject to a more systematic and in-depth ML/TF risk assessment. In the absence of a structured methodology for risk assessment and its effective adoption, improving ML/TF risk management in the real estate sector remains difficult to achieve.

433. *Business centres'* understanding of ML/TF risks remains very low, despite their significant exposure to ML schemes. The general survey carried out in 2022 by SPF Economy highlighted major shortcomings: 66% of business centres have no procedures in place to screen high-risk transactions, meaning they are unable to identify suspicious transactions; and 57% have not carried out individual risk assessments, revealing a lack of understanding of the vulnerabilities specific to each entity and customer. These results reflect a systemic lack of structure in the application of AML/CFT obligations, leaving the sector vulnerable to the use of shell companies and opaque structures for ML purposes. SPF Economy has also noted that many business centres consider that they face no ML/TF risk. This misperception hinders the implementation of appropriate due diligence measures and the adoption of good practice in risk assessment. Some service providers are risk-averse and avoid working with clients with dubious profiles. These divergent practices show that a significant proportion of players do not take any protective measures against potential abuse by criminals.

434. *Notaries* are highly aware of the ML/TF risks associated with their activities, particularly in company creation and property transactions. Both small and large notary firms have a good understanding of the risks associated with opaque structures and multiple transactions, which enables them to implement adequate risk analyses. The support of the National Chamber of Notaries, the 2021 SRA and the typologies are seen as essential resources in their compliance efforts. Notaries express an increased need for up-to-date information on emerging risks.

435. *Lawyers'* understanding of risk varies. Some firms, particularly medium-sized and small ones, demonstrate a good understanding of the risks and incorporate systematic analysis into their practices. However, some large, high-risk firms demonstrate insufficient understanding, focusing more on anonymous transactions and reputational risks while underestimating ML/TF indicators and typologies. AML/CFT supervision reveals significant shortcomings (see below), including a lack of firm-wide risk assessment and individual risk assessment for clients or files, which is a significant weakness for a profession exposed to complex transactions.

436. *Chartered accountants* have a limited understanding of the risks and vulnerabilities specific to their profession. Although the sector has a good theoretical understanding of the high-risk areas it supports

(hospitality, construction, etc.) and professionals have tools to consolidate this knowledge, including SRAs and risk identification models prepared by the ITAA, the analysis of ML/TF schemes related to their services does not appear to be sufficiently thorough.

437. *Statutory auditors* have a better understanding of the risks thanks to more detailed internal analyses. The sector also carries out in-depth risk analyses at the individual level, particularly in large and medium-sized firms where IT tools are used to ensure that clients are monitored on an ongoing basis.

438. Gambling operators (casinos) demonstrate an excellent understanding of ML/TF risks and are attuned to the vulnerabilities identified in the NRA, even though they have not yet received the official version. Casinos have extensive experience in risk management, with most operating for more than 20 years. They use detailed risk analysis, taking into account new technologies (deepfakes, AI) and their implications for fraud, suspicious behaviour, particularly non-betting or interconnected players, and specific profiles of high-risk customers, such as PEPs and certain foreign players. Casinos benefit from automated risk assessment tools, which strengthen their ability to identify and monitor high-risk customers. Some operators have indicated that they maintain active monitoring based on information published by financial and supervisory authorities, such as the BNB and the CTIF, as well as regulatory practices in other jurisdictions. In addition, some have adopted proactive measures to mitigate risks, including prioritising card payments and limiting the use of cash. However, it is not clear whether these good practices are widespread across the sector.

4.4. Understanding and compliance of DNFBPs with AML/CFT obligations and mitigating measures

4.4.1. Customer due diligence, record keeping, BO information and ongoing CDD

439. DNFBPs have a basic understanding of their due diligence obligations. However, there are still significant gaps in their implementation, particularly in high-risk sectors such as for diamond dealers, real estate agents, business centres and certain legal and accounting professionals. The application of due diligence measures varies considerably across sectors, in terms of the scope of supervision, the degree of monitoring and the nature of the documents collected.

440. In most cases, DNFBPs simply check the customer's identity card using a questionnaire, the content of which varies greatly from one sector to another. However, many professionals simply fill in the questionnaire without carrying out in-depth checks on the information provided, which weakens the effectiveness of the AML/CFT due diligence and risk detection system.

441. The majority of *diamond dealers* have a limited understanding of their AML/CFT obligations. Although they are aware of certain requirements, particularly those relating to customer information, their implementation remains inadequate and does not always result in effective compliance. When checks are carried out, they are often limited and not always documented, which compromises the traceability and effectiveness of the due diligence system.

442. Diamond dealers focus their due diligence efforts primarily on establishing relationships, verifying the purpose and nature of business relationships, the identity of business partners, and in some cases, the source of funds. These verifications are generally more rigorous in large international companies, while smaller structures often apply less stringent due diligence. In practice, some choose not to work with unknown or high-risk partners, particularly in the absence of referrals or connections. However, this due diligence diminishes considerably once the relationship has been established: long-standing customers and partners are rarely subject to reassessment, as they are perceived as low-risk. This static approach, based on long-standing trust rather than continuous reassessment, is a significant weakness in the

implementation of due diligence obligations, limiting the ability to detect atypical behaviour or changes in profile over time.

443. SPF Economy has identified major shortcomings in the application of AML/CFT obligations by diamond dealers in the supervised companies selected on the basis of risk. These shortcomings include the systematic failure to identify and verify customers, agents and BOs, as well as a lack of documentation on the purpose and nature of business relationships. In addition, SPF Economy has identified cases of evasion of sanctions, illustrating the sector's vulnerability to illicit financial flows and criminal networks. To address these shortcomings, an AML Policy was drawn up in 2020 and updated in 2024, incorporating detailed guidance and an operational checklist. However, its effective adoption and impact on practices remain to be seen, requiring rigorous monitoring of its implementation.

444. *Business centres* have limited knowledge of their AML/CFT obligations, and show major shortcomings in their implementation. SPF Economy confirmed this during its inspections, which revealed a particularly high non-compliance rate – nearly 71% – in the application of due diligence measures (see next section). The most critical shortcomings concern the lack of verification of clients (41%), agents and BOs (45%), as well as insufficient documentation of business relationships and transactions (45%). Furthermore, the absence or incompleteness of transaction analyses and file monitoring prevents effective monitoring of high-risk financial flows. Service providers that use tools such as ORIS – approximately 6.8% – generally implement their due diligence obligations appropriately. This disparity shows that the use of technological means improves compliance, but that their use remains too marginal to have a significant impact on the sector as a whole.

Table 4.3. Shortcomings noted in the 2022 general survey of business centres

Topic of inspection	No. of entities inspected	Shortcomings noted	
		Number	%
Registration	147	89	60.5%
AML/ CFT obligations	147	104	70.6%

Source: SPF Economy

445. *Real estate agents* are making progress in their understanding of AML/CFT obligations, but this progress remains highly variable and depends on the tools used. The ORIS tool, when used, significantly improves compliance: a general survey by SPF Economy in 2021 revealed that 94% of agents using ORIS complied with basic obligations. However, this tool remains underused in the sector, limiting its overall impact on improving practices.

446. Structural shortcomings remain a concern, particularly with regard to verification of customers and analysis of transactions. Real estate agents have a superficial understanding of AML/CFT obligations, often limited to formal customer identification. In practice, they generally rely on standardised lists of questions, without really investigating or verifying the identity of customers and BOs. Transaction analysis, although carried out, is often insufficient, as understanding of ML schemes specific to the real estate sector remains too superficial. This increases the sector's vulnerability to illicit financial flows, particularly through the undervaluation or overvaluation of property and purchases by nominees.

447. *Legal and accounting professionals* implement vigilance measures which, although generally compliant, vary in terms of effectiveness and systematic application. On the whole, they identify customers and BOs, often by consulting the BO register, although they recognise its shortcomings (see IO 5). Some operators, in particular notaries, chartered accountants and statutory auditors, supplement this verification by cross-checking information with third-party tools and targeted questions on the purpose of transactions and the origin of funds. Chartered accountants and auditors, who have dedicated IT solutions at their

disposal, regularly monitor and update client information, although the use of these tools is sometimes perceived as complex. If the risk is deemed too high, some (chartered accountants, statutory auditors[127] and lawyers) may refuse to enter into a business relationship, an approach that helps mitigate risks but is applied to varying degrees across professions.

448. However, there are significant disparities between professions and between different sizes of firms. While notaries and accountants appear to take a proactive approach, lawyers in small and medium-sized firms have shortcomings in customer identification and the implementation of AML/CFT obligations. Some do not systematically verify the identity of repeat clients and do not always have clear procedures for accepting cases.

449. Since 1 January 2025, it has been easier for lawyers to check that a separate third-party account is held for all transactions involving funds belonging to third parties, thanks to an automatic detection system for atypical payments. This system enables risk situations to be identified in real time and makes it easier to declare or report them to the relevant authorities. No figures are available to date, as the system is too new to allow a quantitative assessment.

450. Finally, *notaries*, who are required to perform certain acts that they cannot refuse,[128] such as the creation of companies, send notifications to the CTIF in case of suspicion, which helps to strengthen the CTIF's analysis in detecting ML. The effectiveness of reports by legal professionals depends largely on their ability to identify ML/TF patterns, a challenge that persists and requires ongoing outreach and awareness-raising efforts by all stakeholders.

451. The *casino* sector benefits from a rigorous framework, supported by a sophisticated automated system (itsme) that facilitates the identification, verification and registration of customers. This system enables real-time monitoring of players, identifying links between them and helping to detect potential ML strategies based on cross-transactions. Operators also have advanced control mechanisms at their disposal, enabling them to carry out additional checks and automatically block access to players who do not meet the compliance criteria, in particular PEPs whose identity has not been properly verified. Casinos also ensure that BOs are identified where necessary. However, without regular supervision and thorough assessment by the supervisory authority, it is impossible to ensure that the AML/CFT measures put in place by the sector are rigorous and adequate.

4.4.2. Enhanced or specific measures

452. Although DNFBPs are aware of their enhanced due diligence obligations, their understanding and implementation remain largely inadequate. Most do not understand the distinction between the different categories of due diligence, particularly with regard to PEPs, high-risk countries and international sanctions, which leads to misinterpretation and partial implementation of obligations.

453. High-risk sectors, including diamond dealers, real estate agents and business centres, have significant shortcomings in their understanding of PEPs. As a result, verification of the PEP status of the customer or its BO is rarely updated after entering into a business relationship, exposing these sectors to the risk of not detecting a change in status. Furthermore, although these professionals have access to the FATF's lists of high-risk countries, the lack of regular updates and the inconsistent application of supervision limit their effectiveness.

[127] In 2023, auditors refused 638 prospective clients for a variety of reasons, including 100 for reasons at least partly related to AML/CFT and 60 (of the 100) for reasons exclusively related to AML/CFT. The significance of ML/TF risks clearly increased following BAOB inspections, coupled with outreach measures (see, for example, publications on the BAOB website such as the *2022 supervision results* and the *2023 supervision results*).

[128] Notaries, who are public officers bound by an obligation to lend their services, may refuse to perform a deed only in exceptional cases, which do not apply when they have suspicions of ML/TF in a transaction, without prejudice to their duty to report to CTIF.

454. *Casinos* show better integration of specific measures, thanks to automated screening of PEPs and sanctioned countries via the EPIS database. However, the many false positives generated by the system make checks more complex, which could undermine the effectiveness of the system.

455. The *legal and accounting professions* have a good understanding of the obligations relating to PEPs and high-risk countries, but their ability to identify these profiles remains limited, mainly due to a lack of structured access to reliable databases. Many of them rely on manual research, particularly via the internet, which affects the accuracy and consistency of their verifications. Large and medium-sized statutory audit firms correctly identify the existence of PEPs, although appropriate due diligence is not always carried out. This issue has been subject to checks by the BAOB and remedial measures have been ordered.

456. The adoption of new technologies is virtually non-existent in all the sectors assessed. Real estate agents, business centres and diamond dealers in particular have little exposure to virtual assets and digital transaction methods, and some reject these innovations as a precautionary measure, rather than developing the capacity to analyse the risks specific to these new tools.

Table 4.4. Summary of findings on the implementation of due diligence obligations by DNFBPs

Sector	Understanding of PEP risks	Verification of at-risk countries	Continuous monitoring	Use of new technologies
Diamond dealers	Limited (checks on entry into the business relationship only, no updates)	Access to FATF lists but updating and application varied	Very limited and irregular (after the initial relationship)	Non-existent (low tolerance of digital innovations)
Real estate agents	Very limited (customer declarations not checked)	Confusion over obligations; few checks.	Virtually non-existent (no follow-up after entry into the business relationship)	Non-existent (few international customers, lack of knowledge of new tools)
Business centres	Low (only those using ORIS carry out checks)	Rarely applied	None, except for companies using ORIS	Very limited (rejection of new technologies as a precaution)
Casinos	Good (automatic filtering via EPIS but false positives)	Systematic via EPIS but cases of false positives	Present but affected by false positives	Good (but needs improvement)
Legal and accounting professions	Fair but incomplete (lack of access to reliable databases)	Good understanding but limited use of specialist tools	Irregular (mainly manual)	Rare (mainly manual checks via the Internet)

Source: Evaluation team

4.4.3. AML/CFT reporting obligations and tipping off

457. Reporting activity, although stable, varies greatly from one sector to another, with relatively high reporting levels among auditors, notaries, chartered accountants and casinos (these four sectors accounted for more than 90% of all reports in 2024). However, it remains very low among lawyers (14 STRs) and in sectors classified as higher risk, particularly estate agents (31), diamond dealers (1) and business centres (14).

458. The situation is particularly concerning for diamond dealers, whose number of STRs was already very low in the previous assessment and has continued to fall over the last five years due to a general decline in transactions caused by COVID-19, G7 sanctions affecting certain diamond-producing countries and the transfer of activities to other international centres. In addition, reports from a number of sectors, including high-risk sectors such as diamond dealers, but also real estate agents and business centres, lack relevance and precision, which limits their added value in detecting suspicious transactions. Even in sectors

where reporting activity is higher, such as notaries, the majority of STRs are not based on genuine ML/TF suspicion, but on a legal obligation to report objective information (use of cash in a real estate transaction; absence of the financial account from which the sum was or will be transferred; identity of the account holders in the preliminary sale agreement or deed of sale).

Table 4.5. DNFBP reporting activity (2020– 2024)

	2020	2021	2022	2023	2024
Notaries	1.177	1.214	1.653	1.150	824
Gambling establishments	157	191	291	322	173
Accounting and tax professions	254	314	319	317	337
Statutory auditors	38	86	84	88	69
Real estate agents	37	48	51	39	31
Business centres	27	19	25	21	14
Lawyers	17	8	14	14	14
Diamond dealers	4	5	3	2	1
Other DNFBPs [129]	43	63	145	106	85
Total					***1548***

Source: CTIF

459. The case of *lawyers* raises a specific issue related to the reporting formalities imposed by law, which require that STRs be sent to the president of the bar, who then forwards them to the CTIF[130]. These formalities, which mainly involve verifying that the suspicion falls within the scope of AML/CFT and that the STRs drawn up by lawyers do not relate to information covered by professional secrecy, add an intermediate step, and associated delays. Presidents of the bar are required to inform the lawyer when the report has been forwarded, but this requirement is not always enforced. This lack of transparency (or feedback to reporting lawyers) may weaken the system, as reporting lawyers do not know whether they benefit from legal protection, which may discourage them from submitting STRs. Furthermore, as in 2015, the reporting rate to the CTIF remains extremely low, despite the potential for identifying high-risk transactions, particularly in the context of complex financial arrangements and real estate transactions. These arrangements are compounded by the absence of any obligation for lawyers to report attempted suspicious transactions (see R. 23 in the TC Annex).

460. The reporting activity of *chartered accountants* is generally satisfactory.

461. In general, and across all sectors, a lack of feedback from the authorities, particularly from the CTIF and SPF Economy, is a factor that weakens the reporting system (see RA d) of IO.6). DNFBPs receive very little feedback on the relevance of their reports, which limits their ability to refine their detection criteria (see IO.6). DNFBPs that have never submitted a STR do not seem to be familiar with information protection measures when transmitting a report to the CTIF. This lack of knowledge, out of fear of compromising confidentiality or exposing themselves to reprisals, can be a significant obstacle to reporting. Some DNFBPs express fears for their safety if they report and seem to misunderstand the existing protection mechanisms.

462. Furthermore, the application of proportionate and dissuasive disciplinary sanctions for breaches of reporting obligations is a major concern (see section 4.6 for more details).

[130] Art. 5, 28° and 53 2017 AML Law

4.4.4. Internal controls, procedures and audits to ensure compliance

463. The effectiveness of internal controls and compliance procedures varies considerably between different sectors of DNFBPs. While some sectors have structured their compliance systems, particularly large firms, casinos and certain legal and accounting professions, others have major shortcomings. The mutual evaluation recognises the need to take into account the scale of DNFBPs' activities and the size of reporting entities in the organisational and supervision requirements of the AML/CFT system.

464. Among the sectors showing high compliance, casinos have internal procedures to ensure the diligence of their employees, but the actual effectiveness of these procedures has not been verified by the supervisory authorities. The *accounting and legal professions* are better structured, with an AMLCO generally appointed, at least in the largest entities, updated compliance procedures and more systematic training. Some notaries have strengthened their compliance by appointing an independent individual dedicated to AML/CFT. Policies and procedures are also more robust. *Chartered accountants*, for example, have detailed policies and procedures, although some note that they are too long, too complex and difficult to apply. In some law firms, double validation of financial transactions has been introduced, and procedures are updated annually, with increasing efforts towards computerisation to enhance their effectiveness.

465. However, in most sectors with a high risk of ML/TF, including diamond dealers, real estate agents and business centres, internal controls are weak or non-existent. Few formal policies and procedures are in place, updates are rare, and training remains inadequate. While recognising the need for a degree of flexibility to take account of the size of the entities subject to regulation, business centres present a particularly concerning level of compliance, with a lack of coordination of the compliance function (only the largest have an AMLCO), while their procedures are often absent and their purpose misunderstood, despite the high level of risk. Real estate agents, with the exception of those using the ORIS tool, apply partial and informal supervision, often reduced to simple questionnaires provided by the IPI, which appear to be poorly understood (see section 4.1).

466. Many sectors do not provide regular, in-depth AML/CFT training, which hampers the effectiveness of their systems. Others appear to offer several training courses, but these do not always seem to meet customer needs, as several sectors continue to have great difficulty understanding AML/CFT obligations.

467. Furthermore, the supervisory authorities do not always systematically assess the actual implementation of internal controls (on the contrary, it would appear that the BAOB always takes internal controls into account in its approach). This lack of monitoring increases uncertainty as to the compliance of entities and limits the possibilities of correcting identified shortcomings.

4.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

468. The evaluation team did not identify any major obstacles to the implementation of obligations and mitigating measures.

4.5. Supervision and monitoring of DNFBPs by supervisory authorities using a risk-based approach

469. The authorities supervise all sectors, with the exception of casinos, where supervision is not effective (see section 4.1). However, for most sectors, this supervision is superficial, often limited to formal checks of documentation, without assessing the practical implementation or effectiveness of the measures put in place to prevent ML/TF.

470. SPF Economy (the "ML/TF prevention" unit) is responsible for supervising more than 15,000 DNFBPs, including high-risk and high-importance sectors such as diamond dealers, real estate agents and business centres, in addition to monitoring compliance with cash payment limits in all businesses in Belgium (see IO 1). Yet it only has 16 FTEs, including three vacant posts in 2023 and part of 2024. Although this unit is supported by a few regional inspectors, human resources remain very insufficient given the supervisory requirements of such a large and high-risk area. The majority of reporting entities do not sufficiently understand their AML/CFT obligations (see section 4.4), making rigorous follow-up all the more crucial. Although staff numbers have doubled since 2015, new control measures have been introduced and new sectors have been made subject to supervision (notably business centres in 2019), as well as a number of other sectors not covered by the FATF Recommendations, such as tax advisers, professional football, art and antique dealers, art and antique storage facilities and safe deposit box rental companies (see the Introduction and IO 1). In addition, the tasks of SPF Economy's AML/CFT prevention unit go well beyond the scope of AML/CFT and include areas as diverse as the supervision of subsidies in the context of military and aeronautical contracts, the supervision of the sale of explosives precursors and the import of conflict minerals, as well as assisting the European Anti-Fraud Office (OLAF) with its supervision on Belgian territory. This dispersion of resources prevents the unit from focusing all its efforts on supervising DNFBPs, which are already under-resourced. Finally, although SPF Economy is attempting to adopt a risk-based supervisory approach, this varies from sector to sector and is not yet fully developed.

471. For *diamond dealers* - the monitoring approach uses a sophisticated scoring tool to identify the highest-risk entities. In 2024, nearly one-third of entities are classified as medium or high risk, confirming the sector's significant exposure to ML/TF risks, while 114 diamond dealers (approximately 8%) are considered high-risk, requiring increased vigilance and enhanced supervision. The frequency of on-site inspections is irregular, with a marked decline in 2022. Only four inspections are carried out per year on average, which is insufficient in this high-risk sector, especially since 76% of the entities inspected present AML/CFT shortcomings.

Table 4.6. AML/CFT supervision among diamond dealers

	2020	2021	2022	2023	2024	Total
Number of inspections	4	7	1	5	4	21
Number of entities with breaches	1	5	1	5	4	16 i.e. 76%

Source: SPF Economy

472. Supervision is performed by specialised inspectors and frequently reveals major shortcomings, which systematically result in financial penalties. The authorities conduct in-depth preliminary analyses (of transactions and networks), making inspections particularly demanding, ranging from three to six months depending on the complexity of the cases. Supervision revealed major shortcomings (see previous section), including a lack of risk analysis, no AML/CFT officer and inadequate customer and BO verification. Due to a lack of resources, no follow-up supervision was carried out and no random inspections of medium- or low-risk entities were conducted. This partial coverage of a high-risk sector limits SPF Economy's ability to ensure effective AML/CFT compliance by diamond dealers.

473. Faced with a lack of resources and in the interests of efficiency, SPF Economy combined its supervision of real estate agents' AML/CFT obligations with the supervision of consumer protection obligations and other legislation falling within its remit as part of a sector inquiry in 2021 and open source research. However, this approach remains insufficient to ensure systematic and in-depth monitoring of ML/TF risks. In 2019, targeted action on luxury real estate, commercial real estate and second homes abroad revealed a non-compliance rate of 78%, but was not followed up systematically due to a lack of resources

In 2021, a general survey showed that 44% of the 334 agents inspected presented at least one AML/CFT breach. Although supervision carried out between 2020 and 2021 confirmed weaknesses, it did not systematically target the most at-risk entities. Between 2020 and 2023, only 37 AML/CFT inspections were carried out, excluding the general survey (see table). Of these inspections, 26 revealed at least one breach, representing a non-compliance rate of nearly 70%; and 7 of the 37 were follow-up inspections in B2B, which is insufficient given the persistent weaknesses in the sector. These figures confirm the significant shortcomings in the sector and highlight a lack of effective coverage, given the scale of the risks identified.

Table 4.7. Supervision of real estate agents (excluding general survey)

	2020	2021	2022	2023	2024	Total
Number of inspections	5	18	7	7	x	37
Of which with breaches	3	12	4	7	x	26 i.e. 70%

x:data not provided

Source: SPF Economy

474. The supervision of *business centres* has evolved towards a more risk-based approach, particularly since 2021. SPF Economy determines which entities to supervise on the basis of fixed criteria, including the concentration of companies at the same address, risky activities, their profile and the frequency of address changes. These elements are supplemented by information from other authorities, including the public prosecutor's office, the judicial police (see *Company Dumping* project, IO 5), the Special Tax Inspectorate (ISI) and other inspection services and authorities with which the Inspection Department of SPF Economy is in contact. A supervision plan is drawn up at the beginning of the year, adjusted according to available resources, with enhanced follow-up for large service providers.

475. In 2022, SPF Economy conducted a sectoral survey of 165 entities, with the main aim of checking unregistered business centres. The results give cause for concern: 57% were not registered and nearly 69% had serious shortcomings (lack of risk analysis, superficial customer checks and poor understanding of AML/CFT obligations). These results demonstrated SPF Economy's ability to detect and sanction unregistered business centres. The pace of inspections has since slowed, with eight inspections carried out in 2024. The low volume of inspections and the high rate of non-compliance detected demonstrate that there is still insufficient understanding of AML/CFT obligations within the sector (see section 4.3). Furthermore, the growing importance of ensuring that business centres are registered and apply appropriate AML/CFT measures is putting additional pressure on SPF Economy, which is already under-resourced, further limiting its ability to supervise the sector.

476. The provincial chambers of *notaries* apply partially risk-based controls, targeting the high-risk activities of each notary (a sample of real estate files and files relating to the incorporation of companies). All notaries are supervised on a three-year cycle by supervisors from within the profession, using a standardised form focusing on customer identification and unusual transactions. However, these inspections are brief (1 to 2 hours), which raises questions about their actual depth. They are rarely announced, which ensures that they are carried out in real-life situations. Finally, in some smaller provinces or districts of Belgium where notaries are more closely connected and professional ties may exist, it might be useful to consider entrusting supervision to notaries from another province or district in order to ensure the necessary neutrality. Furthermore, although supervision did not systematically result in formal reports of breaches, shortcomings in the understanding and application of AML/CFT obligations among notaries were identified, particularly with regard to enhanced due diligence measures (see section 4.4).

477. For *lawyers*, AML/CFT supervision varies across bars, with differing approaches: some rely on risk-based questionnaires, others on random inspections or inspections proportional to the size of the bar. A

single law firm may be registered with several bars, which complicates compliance and supervision. Risk-based AML/CFT supervision, which is still recent (since 2023), is often linked to supervision of quality accounts. For the rest, inspectors check for the existence of measures such as AML/CFT policies and procedures, but focus little on their effective implementation. The resources allocated are generally sufficient, but support from the bars remains variable, with some failing to make recommendations following their inspections. Large firms are generally better prepared, although shortcomings are sometimes noted, while small and medium-sized firms more frequently present shortcomings, particularly in preventive measures and understanding ML/TF risks.

478. The ITAA carries out rigorous AML/CFT supervision of accountants, combining document-based and on-site inspections through several mechanisms: AML investigations, quality reviews, thematic inspections and additional reviews. With 92 inspectors, the ITAA has strong supervisory capacity, enabling it to carry out a large number of supervisory activities. In 2024, it carried out 549 quality reviews, which are conducted every seven years and include a comprehensive AML/CFT component. These activities are complemented by thematic and follow-up inspections. Before each inspection, a document analysis is carried out to identify high-risk firms. On-site visits take an average of 1.5 days, longer for larger structures. In the event of a major breach, follow-up is planned within three to six months. While serious breaches are rare, recurring shortcomings mainly concern information on BOs (incomplete information).

479. The BAOB conducts rigorous supervision of statutory auditors, with robust on-site inspections every three or six years depending on the type of engagement, including a risk-based AML/CFT component. This supervision is combined with thematic inspections that examine how well auditors apply the standards based on the BAOB's risk assessment and the individual risk profiles for each auditor that the BAOB sets up and updates every year. Thematic inspections tailored to the risks are also carried out. With extensive powers comparable to those of the FSMA, the BAOB can intervene effectively in the event of breaches and works closely with other authorities, including the CTIF, particularly when an auditor is deemed insufficiently qualified for certain tasks, such as the verification of virtual asset service providers or in cases of fraud.

480. The CJH does not have the autonomy to hire its own staff, as this is the responsibility of the Ministry of Justice. It employs just five people to oversee a sector comprising some 7,000 establishments (casinos and gambling venues). This structural shortcoming limits the CJH's ability to carry out effective AML/CFT supervision in casinos and gambling establishments, which are inherently exposed to a high risk of laundering.

4.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on DNFBP compliance

481. The authorities have a number of remedial measures and sanctions at their disposal, but often favour an educational approach focused on support rather than sanction. However, awareness remains insufficient, as many reporting entities do not fully understand the importance of implementing effective AML/CFT measures and are not familiar with their obligations. In general, the supervision and follow-up carried out by the authorities remain limited or do not sufficiently target AML/CFT issues. The impact of these actions varies across sectors but remains superficial overall.

482. SPF Economy has stepped up its application of administrative fines since 2019, targeting in particular diamond dealers, real estate agents and business centres. Their impact on compliance in these sectors is significant for the entities sanctioned, but limited for the sector as a whole, due to the low number of sanctions and their lack of visibility. Between 2022 and 2024, nine administrative fines (for AML/CFT breaches) totalling EUR 539 226 were issued to *diamond dealers*. These amounts are deemed proportionate. However, their deterrent effect remains limited, as the sanctions were published

anonymously and the diamond dealers themselves do not appear to be aware of them, thereby reducing the impact on compliance in the sector.

483. SPF Economy notes an improvement thanks to the *AML Policy* for the sector updated in 2024 and training conducted with the AWDC, but these initiatives remain poorly integrated, including among sanctioned diamond dealers. Shortcomings in the understanding of AML/CFT obligations within the AWDC also limit its outreach role.

484. Following the 2021 supervision campaign among real estate agents, SPF Economy issued 53 warnings and 95 fines, which constitutes very significant supervisory action. These proportionate and dissuasive sanctions have prompted some real estate agents to strengthen their compliance, particularly in high-risk sectors (e.g. three agencies operating in the B2B sector, inspected in 2019 and re-inspected in 2023, had improved their compliance). However, these sanctions had only a one-off effect and did not have a structural impact on the sector as a whole. Real estate agents' understanding of ML/TF risks remains very limited, and levels of non-compliance remain high in the sector (see section4.4). The tools available, such as ORIS, are only rarely used, which limits their impact on improving practices in the sector.

485. The impact of SPF Economy measures on the *business centre* sector is more difficult to measure. The 2022 survey revealed that 57% of the entities inspected presented breaches, leading to numerous warnings and administrative fines. These sanctions prompted some service providers to improve their compliance and, in one specific case, to completely overhaul their business model and management tools following supervision. However, major shortcomings persist, particularly in the areas of risk analysis, customer identification and supervision of transactions. As mentioned above, the number of breaches identified in 2022 was particularly high (nearly 69%) and resulted in warnings and administrative fines, some of which were imposed the following year. However, the number of fines remains limited. The sharp increase in warnings in 2022 (94) (see table below) is a useful approach to encourage compliance. However, an increase in the number of sanctions in significant cases of non-compliance would help to raise the level of compliance in this sector. The guidance published in 2022 provides a useful framework for the sector, but its implementation remains variable. Difficulties in implementing AML/CFT obligations remain widespread, and supervisory efforts, which are still limited, have not led to significant change across the sector.

Table 4.8. Number of AML/CFT inspections and results concerning compliance with AML/CFT obligations in the business centre sector

	2020	2021	2022	2023	2024	Total
Number of inspections	7 **	20	165	13	10	215
including those with AML shortcomings	*7 (100%)*	*6 (30%)*	*114 (69%)*	*6 (46%)*	*9 (90%)*	*142 (66%)*
Warning	1	3 (15%)	94 ** (57%)	2 (6.5%)	0 (0%)	102
Report	x	3 (15%)	20 (12%)	4 (31%)	9 (90%)	33
AML* administrative fines	6	3	2	23	3	37
Total amount of AML fines (€)	2590	3540	2065	43164	2450	57859

Note: Administrative fines are calculated according to the year of the decision, not the year of supervision. As a decision may be made in the year following the start of the inspection, this may explain the significant differences between the number of inspections carried out and the number of fines issued in the same year. Five proceedings were still ongoing at the end of 2024.

x: data not provided

** In 2020, SPF Economy introduced a new follow-up system for cases. Extracting data from the old system is proving difficult, which means that the figures for 2020 are incomplete. Some of the inspections carried out that year were only recorded in the old system.

Source: SPF Economy

486. The supervisory authorities for the *legal and accounting professions* can apply disciplinary and sometimes financial penalties. With regard to the legal professions, the authorities favour an educational approach focused on support rather than coercive measures. Although this strategy aims to improve compliance by reporting entities, it limits the deterrent effect of sanctions and does not always seem to guarantee effective implementation of AML/CFT obligations.

487. The provincial chambers of notaries have disciplinary sanctions, but no data could be consulted, making it difficult to assess the sanctions. Since 2023, they have been published anonymously, which means that notaries can now access them. However, anonymity reduces the positive impact. The National Chamber of Notaries has the power to apply sanctions and administrative measures. These sanctions are published in a non-anonymised form but are rarely used and have little deterrent effect. One example is a notary who was fined EUR 15,000 in 2022 for serious offences, including disclosure of a STR submitted to the CTIF and breaches of due diligence obligations. Despite this sanction, he continues to practise and his case has been referred to the public prosecutor's office, raising questions about the effectiveness of the disciplinary system.

488. The bars have never issued financial penalties against *lawyers* and very few disciplinary investigations are carried out. Some investigations have been ongoing for several years in some bars, while other bars have not recorded any cases. The limited number of corrective measures issued, combined with the absence of recommendations in monitoring reports (a shortcoming identified in the previous section), contrasts with the shortcomings observed in the sector's understanding of AML/CFT obligations, which is a cause for concern. Although the authorities report that breaches are generally corrected within the required time frame, the rarity and slowness of proceedings raise questions about the effectiveness of the supervisory system.

489. The ITAA applies disciplinary sanctions (reprimands, suspensions, deregistration) to members who fail to comply with their obligations, including ML prevention measures, which are published on its website.[131] In recent years, it has mainly imposed suspensions of up to three months. It can also impose fines on chartered accountants, but does not have a clear methodology provided for by law for applying and collecting them. This weakens the deterrent effect of the system.

490. The BAOB has good administrative measures in place. For example, the following measures were applied by the Board in 2023 for AML/CFT breaches identified during periodic inspections. For auditors supervising PIEs, 22 measures were taken (reminders, orders, deadlines for corrective action, recommendations and points for attention), and for auditors supervising non-PIEs, 29 measures were taken.

491. The authorities consider that their awareness-raising efforts have an overall positive effect, particularly on customer identification and record keeping. However, shortcomings remain and call for further action. Among *notaries*, the authorities have observed improvements over the past three to four years: better structured internal procedures and more systematic training; some firms have even created a dedicated AML/CFT function to ensure more rigorous and independent verifications and thus prevent notaries who have known their clients for a long time from limiting their verifications. Notaries say they appreciate the publications on the eNotariat intranet and those of the National Chamber.

492. However, shortcomings remain, particularly in the application of enhanced due diligence measures (see section 4.4). Notaries are calling for more practical tools and targeted training. For *lawyers*, the Bar Associations have provided a range of training and compliance support tools, including workshops, webinars and practical tools (such as the Fil Blanc), which are considered useful. They also provide templates that reporting entities can use to implement AML/CFT measures. Some bars, depending on their size, also

[131] https://www.itaa.be/fr/mesures-art118-lab/

organise their own training or call on their Bar Association to provide on-site training. The impact of this training remains limited as significant shortcomings persist in the understanding of AML/CFT obligations.

493. *Chartered accountants* receive good support, particularly through the BE EXCELLENT tool (which is highly appreciated) and active support from the ITAA. The ITAA assists small firms, in particular by allowing the internal whistleblowing channel in small firms (which cannot guarantee the anonymity of the complainant) to be replaced by the use of the ITAA's external whistleblowing channel by the firm's employees. As regards training, firm employees must undergo AML training at least once every three years and, in the case of new employees, within six months of taking up their duties. However, small firms express a need for additional training and more appropriate tools to improve their compliance.

494. For *auditors*, the IRE provides useful information and training to its members. The BAOB provides general guidance and notes a gradual improvement, although small firms still express specific needs for training and appropriate tools. The BAOB has also informed the sector of the information resources available to help identify types of ML.

495. Finally, in the *casino* sector, the BAOB is carrying out outreach activities, but due to a lack of sufficient human resources and effective monitoring, their impact cannot be fully assessed.

5 Transparency and beneficial ownership

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this chapter are R.24-25 and elements of R.1, 10, 22, 37 and 40.[132][133]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) The Belgian authorities have a general but sometimes uneven understanding of the risks associated with legal persons. Their misuse has been identified as a major ML risk and a lesser TF risk. The specific risks associated with foreign legal entities and arrangements with sufficient links to Belgium are not adequately assessed.

b) The reforms introduced by the Belgian Companies and Associations Code (Code des sociétés et des associations – CSA) in 2019 have increased the vulnerability of legal persons by facilitating the creation of shell entities and shelf companies used in ML schemes. The risk of legal entities being used for ML purposes is also increased by the possibility of using nominee directors and shareholders, and potentially straw men, which complicates the identification of beneficial owners.

c) The framework in place for collecting basic and beneficial ownership information is based on a multi-pronged approach and the interconnection of different registers. Belgium has introduced mechanisms to prevent the misuse of legal persons and arrangements for AML/CFT purposes, based mainly on registers (e.g. Banque-Carrefour des Entreprises for basic information, beneficial ownership register (UBO)) and the cross-checking of information between different national registers and information held by reporting entities under the AML/CFT regime. Competent authorities have timely access to the information held in these registers, but some sources of information are underutilised, such as the ones held by the tax authorities.

d) The UBO and Banque-Carrefour des Entreprises registers have a solid architecture and are consulted by competent authorities. However, Belgium lacks sufficiently sophisticated mechanisms to ensure that the information contained in these registers are accurate and current.

[132] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

[133] Recommendations 1, 24, 25, and 40 are under review, see the Technical Annex (TC)

The verifications carried out when legal persons are created are essentially formal. No checks on the accuracy of the data are carried out at the registration stage, and subsequent checks remain limited. Notifications by financial institutions of discrepancies between the information they hold and the data in the UBO register are useful to update the information contained in the register to a certain extent. However, they do not constitute a sufficient means of verifying the data.

e) Belgium has implemented a number of measures, including the striking off and dissolution of inactive entities. These measures are a useful means to improve the accuracy and up to date nature of information on legal persons and entities. However, they are insufficient to tackle the successive creation and use of shell entities in ML schemes.

f) Belgian legislation does not allow the creation of trusts or similar legal arrangements. Foreign legal entities may, however, be administered by a Belgian resident or hold assets or rights in Belgium, in which case they are required to register with the Banque-Carrefour des Entreprises and the UBO registers. Nonetheless, Belgium is not in a position to ensure that foreign legal arrangements with links to Belgium actually comply with their transparency obligations. Analyses have recently been launched in collaboration with the tax authorities to examine the completeness and accuracy of the data relating to these entities. However, the results are not yet available.

Key Recommended Actions (KRAs)

Belgium should:

a) Apply risk-based mechanisms for verifying the information to be recorded in the Banque-Carrefour des Entreprises and UBO registers, to ensure their reliability and mitigate the risks of the creation of legal persons for ML/TF purposes (in relation to the technical compliance failings identified in R.24 – see the TC Annex).

b) Accelerate the implementation of ongoing measures to update the registers (e.g. dissolution of shelf entities, processing of the stock of notifications of discrepancies, and targeted checks of data in the UBO register) in order to improve the reliability of the data currently recorded in the registers.

c) Adopt the necessary measures to ensure greater transparency in the use of nominee directors and shareholders to prevent and tackle the abuse of these mechanisms and facilitate the detection of straw men, while developing a large-scale awareness of the risks associated with straw men.

Other Recommended Actions

Belgium should:

a) Deepen its understanding of the types of ML/TF associated with different types of legal person and foreign legal persons and arrangements with links to Belgium, including by involving the prosecution authorities on the basis of cases they have encountered, to develop a more granular understanding of the methods and techniques used to misuse these entities.

b) Simplify the procedures for updating basic information and reduce the costs incurred to facilitate the process and verify that the obligation to keep information current is met.

c) Adopt a faster procedure for dissolving inactive entities, as announced in the AML action plan of March 2024.

d) Implement targeted awareness-raising actions aimed at DNFBPs (especially notaries, estate agents, business centres - company service providers), on the importance of their role in strengthening the transparency of legal persons, and on the red-flag indicators of ML/TF involving the different types of legal entities/arrangements and foreign legal persons with links to Belgium.

e) Take steps to ensure that trusts and similar legal arrangements subject to transparency obligations in Belgium meet these requirements.

f) Use the information held by tax authorities to identify beneficial owners, trusts and legal arrangements and, more generally, for AML/CFT purposes.

g) Adopt and apply sanctions to entities that do not comply with their obligations to communicate and update basic information, or which transmit false information.

h) Incorporate all professional bans into JustBan, including those imposed as part of criminal transaction procedures.

Overall Conclusions on IO.5

Belgium is highly exposed to ML/TF risks related to the abuse of legal persons. The Belgian authorities have a general understanding of these risks of abuse of Belgian legal persons for ML/TF purposes, but this understanding varies between authorities. The specific context of Belgium of polycriminal activities in which the abuse of legal persons occurs is not always well identified or understood by the Belgian authorities. There is insufficient understanding of the risks posed by the use of foreign legal persons, foreign trusts and similar legal arrangements in ML/TF schemes, which is an important weakness, in the country's open economic context.

The introduction of the register of beneficial owners in 2018 is a positive step forward and complements the existing register of basic information on legal persons. These registers allow the competent authorities to access basic and beneficial ownership information in a timely manner. However, significant weaknesses in the mechanisms for ab initio verification hinder the authorities' ability to identify entities created for ML/TF purposes and make the information they access less reliable. The measures implemented only moderately mitigate the weakness of the verification measures taken by the authorities in charge of the registers. This shortcoming is significant in the context of the high risk of ML/TF involving the use of legal persons and legal arrangements in Belgium. The 2019 reform of the CSA has further increased the vulnerabilities of legal persons by facilitating their creation, without sufficient mitigating measures being taken, particularly with regard to the use of straw men and shell companies, which have a known high risk of abuse in Belgium.

Major improvements are required.

Belgium is rated as having a Moderate level of effectiveness for IO.5.

Immediate Outcome 5

496. The evaluation team has based its conclusions on an examination of the documents submitted by Belgium and discussions with the Belgian authorities during the on-site visit.

5.1. Identifying, assessing and understanding ML/TF risks of legal persons and arrangements

5.1.1. Belgian legal persons

497. The Belgian authorities have a general understanding of the ML/TF risks associated with legal persons. Nevertheless, the understanding of some key risks is sometimes inconsistent, especially with regard to important typologies in Belgium such as the use of straw men, shelf entities and certain risks associated with company service providers. Belgium identifies the risk of misuse of legal persons as a major ML risk. The CTIF and the prosecution authorities have a good understanding of the risks and types of use of legal persons for ML purposes. The authorities in charge of the basic information register (Banque-Carrefour des Entreprises register), and SPF Finance-Treasury in charge of the beneficial ownership register (UBO register), have an adequate understanding of the risks. Certain reporting entities, particularly DNFBPs, exhibit a lower level of understanding. Notaries have a reasonable albeit sometimes theoretical understanding of these risks, as do company service providers (business centres, see IO.4), whose awareness appears to be more recent and sometimes approximate.

498. The understanding of ML risks is informed by the ML NRA and a cross-sectoral assessment of the risks associated with legal persons and legal arrangements carried out by SPF Finance - Treasury in 2019 and updated in 2024. The existence of this cross-sectoral assessment is a positive development since the 2015 FATF report. It is based mainly on the ML NRA, the European Commission's supranational ML/TF risk analysis and data provided by the Federal Police Criminal Investigation Department (*Police Judiciaire Fédérale* – PJF), the CTIF and SPF Economy. The prosecuting authorities were not involved. The cross-sectoral assessment provides an overview of the applicable framework, threats and vulnerabilities to which legal entities are exposed in terms of ML and, to a certain extent, TF. It also identifies the main shortcomings in the applicable framework.

499. Overall, the cross-sectoral evaluation is mainly descriptive and lacks granularity in the analysis and on the use of typologies to allow for a more in depth understanding of the methods and techniques used to misuse legal persons. The typologies used in ML schemes linked to high-risk areas, e.g. drug trafficking, tax and social security fraud, diamond dealers, etc., have not been specifically examined. The description of certain *modi operandi*, such as the use of the offsetting system or TBML, is not accompanied by typologies to identify more specific methods of misuse of legal persons. Recent work on Brazilian and Romanian offsetting systems has helped to develop a better understanding of the mechanisms used (see IO.1 and 6). However, the assessment does not include a sufficiently detailed analysis of the Belgian context of polycriminal activities in which the abuse of legal persons takes place.

500. The Belgian legal framework contains an important number of vulnerabilities which the Belgian authorities have identified in the cross-sectoral assessment and which they broadly understand. However, a number of key vulnerabilities need to be further analysed and clarified, including to the use of nominee directors which enable the use of straw men. This issue is mentioned, but the assessment lacks detail concerning the profile, frequency and means of involvement of these straw men in ML schemes.

501. The cross-sectoral assessment considers that the main risks and vulnerabilities affecting legal entities are not specific to a particular legal form. Overall, the assessment identifies simple legal structures as being at risk of abuse but without defining this notion. However, levels of risk are attributed to the various forms of legal person, although they are not always sufficiently documented. General partnerships (*sociétés en nom collectif* – SNC) are identified as the form of company presenting the highest risk of ML, although the mechanisms for using these entities in criminal cases are insufficiently documented.[134] Limited

[134] General partnerships account for 9% of the cases involving legal persons referred to the judicial authorities by the CTIF, even though there are only 29,000 of them.

liability companies (*sociétés à responsabilité limitée* – SRL) are also identified as being at risk due to their prevalence in the CTIF's reports to the judicial authorities and in investigations carried out by the Federal Police Criminal Investigation Department.[135] As far as public limited companies (*sociétés anonymes* – SA)[136] and limited partnerships (*sociétés en commandite* – Scomm) are concerned,[137] certain vulnerabilities have been identified, but they should be better documented and analysed (see the Introduction for a description of the different categories of company). "S*ociétés simple*s" also run the risk of being used as shell companies in complex corporate arrangements. The understanding of the risks exposure of this form of companies differs between certain authorities according to their scope of activity: SPF Economy has identified the risk posed by these entities during inspections of company service providers, whereas the judicial authorities consider that this risk is not corroborated by the judicial records.

502. The risk of TF associated with legal persons is lower than the ML risk. The entities the most at risk are non-profit organisations (*associations sans but lucratif* – ASBL), which are perceived as posing a moderate risk due to their ability to collect and transfer large amounts of funds in high-risk areas. The TF NRA for NPOs (see IO.10) attributes a high degree of vulnerability to the multiplication of ASBLs, which are "dormant/inactive" shelf entities that can be reactivated for TF purposes. The measures taken to deregister and dissolve dormant ASBLs increase the identification of those that are active and, to some extent, reduce the risk of misuse of these entities for TF purposes. However, the Federal Public Prosecutor's Office notes that the direct involvement of a legal person in TF matters is rare to date, based on judicial records. Nonetheless, the understanding of the TF risks appears to be uneven and needs to be improved to ensure that it is firmly rooted in the country's risk context.

5.1.2. Foreign legal persons and arrangements

503. The Belgian authorities' have a limited understanding of the risks to which Belgium is exposed from foreign legal entities. The open nature of the Belgian economy and the country's European and international connections (see the Introduction) mean that close attention should be paid to the risks associated with these entities. The Belgian authorities have not specifically assessed the risks posed by foreign legal entities and arrangements that have links with Belgium. Only the use of "limited liability" companies and legal entities or arrangements based in low-tax countries or territories or free trade zones, in the context of types of ML involving diamond dealers, is identified in the ML NRA. The cross-sectoral analysis also identifies a typology favouring identity concealment involving limited partnerships, in connection with a foreign limited liability company. However, no other form of foreign company, nor any other typology involving foreign legal entities, is considered in the cross-sectoral or national analysis of ML risks.

504. The authorities have identified a total of 66 012 foreign entities with links to Belgium, 7 645 of which have a branch or a unit in Belgium. The other foreign entities that have a link with Belgium are those subjected to various legal obligations in Belgium, such as engaging in activities subject to VAT in Belgium, employing staff subject to Belgian social security, participating in Belgian public procurement contracts, or renting property in Belgium. However, the Belgian authorities consider the materiality of the ML risk associated with these legal persons to be low, given that the 66 012 foreign entities are only a small proportion of the total of 870 410 Belgian legal entities listed at the end of the on-site visit (February 2025) and in the light of the low number of report based on STR involving foreign entities transmitted to the judicial authorities (8% of transmissions involving legal persons are foreign legal persons). However, these

[135] Limited liability companies account for 75% of the cases involving legal persons referred to the judicial authorities by the CTIF and 30% of the investigations opened by the Federal Police Criminal Investigation Department.

[136] Public limited companies account for 6% of the cases involving legal persons referred to the judicial authorities by the CTIF and 6% of the investigations opened by the Federal Police Criminal Investigation Department.

[137] Limited partnerships account for 2% of the cases involving legal persons referred to the judicial authorities by the CTIF.

factors are not sufficient to justify a low level of risk. Foreign entities represent 7% of entities operating in Belgium, and ML cases involving offsetting schemes have revealed the use of foreign entities (e.g. see the "Clown" case, IO.7).

505. With regard to trusts or similar legal arrangements, Belgium has not ratified the Hague Convention and does not authorise the creation of legal arrangements in Belgium. However, foreign legal arrangements may be administered by a Belgian resident or hold property or rights in Belgium. A person domiciled in Belgium may also be the settlor or beneficiary of a trust governed by foreign law. Finally, these foreign legal arrangements may have effective control over a Belgian legal entity (see Rec. 25 in the TC Annex). The risks associated with trusts and similar legal arrangements in the specific context of Belgium are not identified in the cross-sectoral assessment of legal persons and are assimilated to the risks posed by foreign legal persons. The 2015 FATF report previously noted the lack of measures taken to identify and assess the vulnerabilities of legal arrangements operating in Belgium.[138] The fact that these legal structures are not created in the country makes it difficult to identify them and to understand and assess the risks associated with them. The mandatory UBO registration requirement only allows for the identification of certain entities: 746 foreign legal arrangements registered as intermediate entities of Belgian legal persons. Among these, the Belgian authorities have identified fourteen foreign legal structures administered from Belgium.

5.2. Mitigating measures preventing misuse of legal persons and arrangements

506. Belgium has adopted a series of measures which, taken together, can to some extent mitigate the risks of misuse of legal persons and arrangements for ML/TF purposes. Changes have been made to the legal framework in order to increase the transparency of legal persons and arrangements: (i) the *abolition of bearer shares,* which was introduced in 2005 came into full effect in January 2014; (ii) access to the central register of financial accounts and contracts (PCC) held by legal persons with Belgian FIs and initially set up in 2011 for tax purposes was extended to AML/CFT authorities in 2018; (iii) convictions of legal persons have been centralised in an criminal record effective since 2016, and (iv) company service providers offering corporate domiciliation services became subject to the AML Law in 2018 (see Rec. 22 in the TC Annex and IO.4).

507. The AML Action Plan adopted in March 2024 sets as a priority increasing the transparency of legal persons and legal arrangements (see IO. 1). The 2019 reform of the Companies and Associations Code (CSA) streamlined the legal framework by reducing the number of corporate forms and by consolidating all applicable rules within a single code. However, this reform has also further increased the intrinsic vulnerabilities of the legal framework by easing the conditions for creating entities, thereby facilitating the creation of shelf entities and shell companies used in ML schemes. These changes have led to a significant increase in the creation of limited liability companies – the type of company identified as being more highly exposed to ML risks (see section 5.1.1 above) – accounting for more than 97% of newly-formed companies.[139] This reform sends a strong signal to the priority given to economic considerations over AML/CFT.

[138] MER, para. 7.27, p.139.

[139] In its business barometer published in July 2023, the Belgian Federation of Notaries (Fednot) noted an increase in the number of new businesses, particularly companies, each year between 2019 and 2023, despite the Covid crisis. Around 2,111 companies were created per month in the year prior to the introduction of the CSA in 2019, compared with 3,401 per month in 2023. FEDNOT's analysis also shows that between 2022 and 2023, 97.4% of the companies created were limited liability companies (SRLs), which can be explained by the many advantages offered by this legal form since the introduction of the CSA. For non-profit associations, a positive trend has also been observed in recent years, with the number of ASBLs rising from over 134,000 in 2021 to around 144,500 at the start of 2024.

508. *Registers* - All Belgian legal persons and certain foreign legal persons and entities with links to Belgium must register in the Banque-Carrefour des Entreprises.[140] Since September 2018, Belgian legal persons and foreign legal persons and arrangements administered in Belgium[141] are also required to declare their beneficial ownership to the UBO register managed by SPF Finance, which is a significant development. However, current shortcomings in checking the accuracy of the information provided prevent it from being used as a completely reliable tool (see section5.3 below)

509. A central register of bans imposed against individuals who are prohibited from managing – *interdiction de gérer (JustBan*) was set up in May 2023 to prevent people subject to a ban, imposed as part of criminal or civil convictions, from setting up and controlling entities for ML/TF purposes. The Belgian authorities had found that 50% of persons that had been banned continued to exercise management functions, with 10% of them even taking on new functions, which illustrates the weakness of the checks carried out when new entities were created and when subsequent changes were made (see section5.3). On 30 January 2025, the register contained a total of 3 668 measures. It is freely accessible to the public and notaries and commercial court clerks are required to consult it and must refuse to register directors or managers who are subject to such a ban.[142] This register is a useful tool for ensuring the effective implementation of management bans. However, it does not include bans imposed as part of criminal transactions procedures, which are frequently used by the Belgian criminal justice system (see IO.7). Belgium did not provide data to enable the evaluation team to assess the extent to which this tool has prevented the exercise of managerial functions by persons subject to a ban. The possibility of using nominee directors and straw men also enables criminals to circumvent the bans imposed.

510. *Nominee directors and shareholders* – The concepts of nominee directors and shareholders[143] are not framed in Belgian law. Following a FATF recommendation in 2015, legal persons appointed as directors of another legal person may no longer appoint another legal entity as their permanent representative. The identity of the nominee directors/shareholders must be formalised by an instrument of appointment, filed with the registrar, published in the Belgian Official Journal (*Moniteur belge*) and entered in the Banque-Carrefour des Entreprises register. However, the principal’s identity and the nominee’s status are not made public, which complicates any verification of the principal's capacity. In addition, nominee directors in a professional capacity are not subject to the AML requirements, despite a FATF recommendation in 2015 (also see Rec. 23, IO.1 and 4). The Belgian authorities state that the use of nominee directors remains marginal. However, most ML schemes, particularly those involving offsetting schemes, involve the use of “nominee” directors, particularly when new legal entities are created and registered. The reality of this phenomenon in Belgium was highlighted on several occasions during the on-site visit, including by the CTIF. It is also noted in the cross-sectoral analysis of legal persons in September 2024, which highlighted the risks associated with the absence of a relevant framework in Belgium. These factors constitute a major vulnerability in the Belgian system, and the mechanisms in place do not allow for the effective detection and control of the use of such staw men for ML/TF purposes. The cross-sectoral analysis of legal entities recommends several measures to counter the use of straw men, but they have not yet been implemented.

[140] 66 012 foreign entities have links with Belgium, which requires them to register in the Banque-Carrefour des Entreprises register. 7,645 of these have an establishment or branch in Belgium. Other foreign entities are entered in the Banque-Carrefour des Entreprises register in compliance with the various Belgian laws that require it, such as entities subject to VAT and Belgian social security as an employer, and those that take part in public procurement contracts or rent property in Belgium. Legal entities that are required to submit information to the UBO register must first register in the Banque-Carrefour des Entreprises register.

[141] This applies to subsidiaries whose registered office is located in Belgium and to trusts and legal arrangements whose trustee or fiduciary is established, domiciled or resident in Belgium; whose registered office, principal place of business or trustee’s or fiduciary’s place of management or administration is located in Belgium; which establishes a business relationship or acquires property in Belgium on behalf of the trust.

[142] Legal obligation under Article 13 of the Law of 4 May 2023 on the central register of disqualifications from management.

[143] Shareholders acting on behalf of another person, holding shares registered in the name of nominees

511. *Beneficial ownership identification and verification measures* - FIs and DNFBPs are required to identify their legal person and legal arrangement customers, as well as the beneficial owners, as part of their AML/CFT due diligence obligations (see Rec. 10 and 22 in the TC Annex). These obligations are an additional means of reducing the risks of misuse of these entities. However, some DNFBPs have a partial understanding of the notion of beneficial ownership, limited to holding 25% of the company's shares. This partial understanding of the concept of beneficial ownership reduces the ability of these reporting entities to identify and understand their customers' ownership chains and beneficial owners (see IO.4).

512. *Oversight by notaries when certain legal persons are created* - Notaries do not play a sufficiently active role when new companies are created (see section 5.3). The incorporation and subsequent amendments of five of the nine corporate forms (especially limited liability companies (SRL) and public limited companies (SA), which are the most common types of company in Belgium) require a notarial deed (see the Introduction and Rec. 24 TC Annex).[144] Two of these five companies are seldom used (the European company (SE) and the European cooperative society (SCE)). However, corporate forms with high ML/TF risk are created by private deed (general partnerships (SNC) and limited partnerships (SComm)), as are non-profit associations (ASBL). Notaries are required to consult the *JustBan* register in addition to applying the AML/CFT diligence measures to which they are subject as reporting entities and under which they identify the parties to the deed. However, checks on the company's incorporation documents, such as the financial plan, are essentially formal (checks on the existence of the document, the presence of mandatory information and the number of financial years covered). The applicant is not required to provide proof of the registered office's address, despite the vulnerability of the system identified by Belgium in this respect, and it has been found that in the presence of a nominee, a rigorous verification of the nominator's identity is not always carried out. Therefore, their involvement is not sufficient to guarantee the reliability of the data that they subsequently transmit to the commercial court clerks who register the new entities in the Banque-Carrefour des Entreprises. It does not effectively reduce the misuse of legal persons for ML/TF purposes.[145]

513. *Dissolutions* - Finally, the Belgian authorities identify and dissolve "dormant/inactive" entities registered in the Banque-Carrefour des Entreprises to prevent them from being reactivated for ML/TF purposes.

514. In 2022, the Belgian authorities estimated that around 170 000 entities, including 70 000 ASBLs, registered with the Banque-Carrefour des Entreprises were inactive. The dissolution measures have reduced the number of these entities by almost half. In November 2024, the Belgian authorities estimated that 80 000 inactive entities were still registered in the Banque-Carrefour des Entreprises, 75% of which were non-profit associations. Inactive entities were identified on the basis of breaches such as failure to file annual accounts, register beneficial owners in the UBO register, appoint directors, publish the required documents in the *Moniteur belge*, or failure to comply with the modification of corporate forms following the entry into force of the CSA. The Belgian authorities have also undertaken to analayse data relating to Internet, electricity and telephone subscription contracts to identify inactive entities. However, there has been no systematic use of such data as an indication of inactive entities.

515. The dissolution measures taken by certain commercial tribunals[146] at district level in collaboration with SPF Economy are helping to reduce the number of inactive entities and therefore limit the possibility of reactivating shelf entities, which are already registered in the Banque Carrefour des Entreprises for ML/TF

[144] The creation of three forms of non-profit legal entity also requires an authentic instrument (international non-profit association (*association internationale sans but lucratif* – AISBL), private foundation (*fondation privée* – FP) and public interest foundation (*fondation d'utilité publique* – FUP)).

[145] Two court rulings transmitted by Belgium illustrate the fact that both entities formed by a private deed (SComm) and entities created by an authentic instrument (SA) may be involved in ML schemes.

[146] The registries of the commercial courts are responsible for recording the data in the Banque-Carrefour des Entreprises register and for publication in the *Moniteur belge*.

purposes. However, the risks have since moved, with some entities transferring their head offices to districts that have not yet introduced such measures so as to avoid these checks. In response, commercial tribunals in various districts have launched similar initiatives, although the results are not yet known.[147]

516. These dissolution measures therefore produce certain results (see section 5.5 below) but overall, they remain relatively ineffective due to the length and complexity of the procedures and the limited human and technical resources available. This is in contrast to the relative ease with which head offices can be relocated from one district of Belgium to another, and the simplified procedures for creating new entities, which lead to a significant increase in the number of companies created. Nor are these dissolution measures accompanied by sufficient measures to prevent the creation and use of new shell entities in ML/TF schemes in the absence of sufficient checks when legal persons are created (see section 5.3), a modus operandi that is observed in many offsetting schemes in Belgium. The AML Action Plan includes a proposal to introduce an administrative dissolution procedure for a more flexible and faster procedure (see IO 1). However, this currently remains at the draft stage.

517. Finally, *financial transparency measures*, such as the obligation to file annual accounts for certain types of legal entities (limited liability companies, non-profit associations and foundations), help to increase the transparency of the framework applicable to legal persons and possibly identify potential abuses.[148] However, this obligation to file accounts does not apply to all general partnerships, limited partnerships and ordinary simple partnerships, despite the ML/TF risks associated with these legal forms.[149] The obligation to provide notaries with a financial plan when certain companies are created is not part of an AML/CFT objective but is a measure that is likely to reduce the risks of misuse of legal persons. However, the conditions necessary for this requirement to have an impact in AML/CFT matters have not been met, as the plan does not have to be drawn up by a professional accountant and notaries only carry out formal checks on the documents. These measures can therefore only prevent and identify the misuse of legal persons for ML/TF purposes to a minimal extent.

5.3. Legal persons: Timely access to adequate, accurate and current basic and beneficial ownership information

518. The competent authorities have timely access to the data held in the Banque-Carrefour des Entreprises and UBO registers. However, the current systems do not always guarantee access to adequate, accurate and up-to-date information by the competent authorities.

5.3.1. Basic information

519. Belgium gives an important weight to the role of notaries in ensuring the reliability of basic information registered in the Banque-Carrefour des Entreprises (see section5.2 and Rec. 24 of the TC Annex). However, in practice, their involvement does not constitute a sufficiently effective filter to ensure the reliability of basic information. Notaries are required to collect certain information as part of their due diligence obligations, which improves the reliability of this data. However, notaries only carry out formal checks on the basic information provided to them. They are required to accept the deed requested by the client – except in exceptional cases where the deed is contrary to public order – and do not carry out

[147] In addition to "Company Dumping" in Brussels, this project has been extended to the Halle/Vilvoorde and Walloon Brabant districts, under the same name. The project is called "Lescoop" in Leuven, "Figaro" in Ghent, "Horus" in Mons, "Ghostbusters" in Limburg, and "Kali" in Antwerp.

[148] The obligation to file accounts does not apply to all general partnerships, limited partnerships or ordinary simple partnerships, despite the ML/TF risks associated with these legal forms.

[149] For the filing of accounts for the 2023 financial year, 517 general partnerships and 924 limited partnerships met the criteria requiring them to file annual accounts.

independent checks on the information provided by their clients (see section 5.2). In practice, notaries submit a limited number of STRs to the CTIF relating to the creation or modification of companies, contributing to a small extent to the identification of potential shell companies. The cross-sectoral assessment of legal persons reveals that notaries are sometimes used without their knowledge in ML schemes involving legal persons and that in some cases notaries have played an active and intentional role in these practices. During the period covered by this assessment, one notary was suspended by the Chamber of Notaries and received an administrative fine for failing to comply with the obligation to report suspicions in relation to allegations concerning his involvement in the successive creation of dozens of shell companies. These various factors raise questions about the ability of notaries to identify and report potential signs of legal persons established for the purpose of ML.

520. The clerks of the commercial courts and approved business registration offices (*guichets d'entreprises*) [150], which are also involved in registering newly created entities, have a mainly administrative role and do not carry out independent checks. Only formal inspections are carried out when the data is entered, with the exception of checks on the prohibitions from acting as a director via the JustBan register, which have been in place since 2023. For example, the legal representative is not required to provide proof of the registered office, which allows the use of fictitious or fraudulent addresses for registered offices. As a result, no verification measures are taken for the five types of legal person created by private deed, some of which present high ML risks, apart from the vigilance measures taken by FIs. A circular issued by SPF Justice in October 2023 requires registries to check certain elements, in particular the identity and proof of residence of natural persons (see Rec.24, TC Annex). However, this circular only concerns the filing of paper documents, not electronic files. The practical effects of this circular have not yet been demonstrated.

521. Once the information is recorded by these parties in the Banque-Carrefour des Entreprises register, it is not verified by SPF Economy, which is responsible for the register, nor are requests for additional information made in the event of doubts about the information received before it is made public, unless SPF Economy is informed of a discrepancy. In such cases, Banque-Carrefour des Entreprises may verify, correct or, where necessary, delete the incorrect data.

522. Subsequent changes to the information recorded in the Banque-Carrefour des Entreprises register follow the same procedure as for the creation of a legal person and is subject to the same shortcomings. The Belgian authorities also note that a number of changes are not notified to the Banque-Carrefour des Entreprises register due to practical constraints and the cost of updating the information. These factors do not encourage legal administrators to complete these legal formalities, which undermines the accuracy of the data recorded. This can result in obsolete data remaining in the Banque-Carrefour des Entreprises register without being proactively identified by the Belgian authorities. As a result, there is insufficient assurance that the data is accurate and up to date.

523. A 2020 report by Banque-Carrefour des Entreprises highlighted problems with the quality and accuracy of the information, as well as it being kept up-to-date. In particular, it noted the impact of the lack of accuracy of certain basic information, in particular information relating to the addresses of entities' registered offices.

524. The Belgian authorities rely mainly on notifications received from other administrations, such as the tax authorities, and professions, such as company service providers, and from the police to identify the existence of incorrect data in the register. Between 2020 and 2024, 27 033 discrepancies were notified to

[150] The registries of the commercial courts are responsible for recording the data in the Banque-Carrefour des Entreprises register and for publication in the *Moniteur belge*. Approved business registration offices complete the registration in the Banque-Carrefour des Entreprises register, recording certain data such as contact details, the activities carried out and the bank account. These offices are the only points of contact for registering simple companies in the Banque-Carrefour des Entreprises register. Foreign legal entities must register with Banque-Carrefour des Entreprises in some cases, this registration is also finalised by an approved business registration office.

Banque-Carrefour des Entreprises and 48 918 addresses were deleted. Incorrect addresses are the main reason for discrepancies reported.

525. In addition, technical problems with encoding information in the register affect the accuracy of information and access to it by the competent authorities.[151] Encoding errors can be made and delays are sometimes observed in the entry of information by the registry.[152] Finally, the accuracy of information recorded is also affected by delays in adjusting statutes and converting the legal forms of certain companies following the entry into force of the CSA. At the end of the on-site visit (February 2024), approximately 13.55% of the entities concerned by such a change had not yet taken the necessary steps.

526. The Banque-Carrefour des Entreprises register is interconnected with other registers, in particular the UBO register, in accordance with the Only Once principle, which stems from the Law of 5 May 2014 stipulating that a person is only required to provide information to the administration once. This information is then accessible to other administrations through interconnections, with each administration being responsible for the information it collects. Information recorded once is therefore repeated in other databases, ensuring consistency between them. Notifications of discrepancies submitted by reporting entities and competent authorities via the UBO register and the administrative formalities associated with registration in the UBO register have made it possible to identify obsolete data or inconsistencies relating to the basic data of legal persons. However, the lack of verification of data accuracy prior to its recording into the Banque-Carrefour des Entreprises register is a major vulnerability of the system, creating the risk of duplicating errors and inaccuracies in interconnected databases.

527. In conclusion, the competent authorities have timely access to basic information on legal persons recorded in the Banque-Carrefour des Entreprises and in the *Moniteur belge*. The weakness of the *ab initio* verification measures leads to an increased need for *ex post* controls, which do not ensure the accuracy of the data, especially in a context of a significant increase in the number of new entities since the entry into force of the CSA. The competent authorities therefore do not have a reliable tool for accessing basic information about legal persons. In the 2024 cross-sectoral assessment, Belgium identified the need to establish a systematic mechanism at the stage of setting up new companies to prevent the creation of companies by criminals. This shortcoming had already been the subject of a recommendation to Belgium by the FATF in its 2015 evaluation report.[153]

5.3.2. Information on beneficial owners

528. The competent authorities have timely access to information on beneficial ownership via the UBO register. The register has a robust architecture and is interconnected with other national databases[154], which allows for cross-checking of the information provided. The SPF Finance carries out close monitoring to ensure that legal persons declare their beneficial owners and conducts monthly checks to verify the registration of beneficial owners by newly created entities. Registration rates are very high and only 2.21% of entities have not yet fulfilled their obligation to declare beneficial owners. SPF Finance estimates that out of 4 000 entities created each month, around 100 do not register their beneficial owner, which leads SPF Finance to take further action against them (see section 5.5). Foreign legal persons registered in the Banque-Carrefour des Entreprises register are not required to provide information on beneficial owners

[151] Foreign legal persons and foreign trusts and legal arrangements are also registered under a single category, "foreign entities", which does not allow any distinction to be made between them.

[152] NRA of legal persons page 54.

[153] FATF Mutual Evaluation Report (2015), section 7.4, p.145.

[154] The UBO register automatically retrieves certain data from the Banque-Carrefour des Entreprises register, the National Register of Natural Persons and the Banque-Carrefour de la Sécurité Sociale (BCSS). Supporting documents must be provided at the time of registration, unless they have been published in the *Moniteur belge*.

and are therefore not registered in the UBO register, unless they are subsidiaries established in Belgium or if they hold shares or exercise control over entities subject to the obligation to register in the UBO register.

529. Information on beneficial owners is registered on a declarative basis, often through intermediaries (e.g. accountants, solicitors, notaries), without the SPF Finance, which is responsible for the register, verifying the accuracy of the data provided. Only technical restrictions are in place at the registration stage to avoid formal errors or certain structural inconsistencies in the data entered. The information recorded in the UBO register must be accompanied by supporting documents, which are accessible to the competent authorities. These documents are not subject to verification *ab initio*, but serve as support when any subsequent checks are carried out. This information must be confirmed each year, but this formality is not accompanied by a specific check by SPF Finance to ensure that it is actually completed and that the data provided is accurate. The impact of inaccurate information is important given that the competent authorities consult the register fairly systematically to obtain information on beneficial owners in the course of their duties. In this context, the data used in investigations and prosecutions is potentially inaccurate. Similarly, with the exception of large FIs that use other sources of information, FIs and DNFBPs rely primarily on UBO register data to fulfil their due diligence obligations (see IO. 3 and 4), which potentially increases the risk of dissemination and use of erroneous data if these entities do not carry out additional checks.

530. To address these shortcomings, since August 2024 the SPF Finance has been conducting individual checks on data already recorded, targeting primarily entities presenting risk factors such as: a complex structure, foreign control established or residing in a high-risk third country or tax haven, incomplete control information in the UBO register, the existence of at least two notifications of differences, etc. SPF Finance aims to carry out 1 000 inspections per year, which should be put into perspective with the annual number of new entities created, which is around 48 000 (or approx. 2% of newly created entities). The initiative to introduce risk- based checks is appropriate, although it is still too early to assess their effectiveness. The lack of verification of the accuracy of data *ab initio* automatically leads to an increased need for *ex post* verification, without the Belgian authorities having the necessary resources to check a sufficiently wide range of recorded data, especially given the growing number of legal persons created since the reform of the CSA. As a result, these checks remain insufficient to ensure the accuracy of the data.

531. In practice, a significant part of the burden of ensuring the accuracy of data on beneficial owners rests on the mechanism for reporting discrepancies to the SPF Finance, which certain entities and competent authorities have been required to do since 2021. The multi-pronged approach implemented by Belgium to access information on beneficial owners is based primarily on a combination of the UBO register and this mechanism for reporting discrepancies. Any discrepancies between the information reporting entities have as part of their due diligence measures and that in the UBO register must be reported. These reports of discrepancies mainly come from financial institutions. DNFBPs generally rely on information from the UBO register to identify beneficial owners. Some of them also have a limited understanding of the concept of beneficial owner (see section 5.2). Many of them are unaware of their obligation to report discrepancies. Notaries, lawyers, chartered accountants, statutory auditors and bailiffs are not required to report discrepancies they identify in certain cases, which may also explain the limited number of reports from these professions. [155]

532. On average, SPF Finance received 1 000 notifications of discrepancies per month in 2024 and a total of approximately 32 000 notifications between 2021 and early 2025, involving 12 848 legal persons.

[155] Article 74/1 § 1 of the AML Law. These professions are not required to report discrepancies when the information and intelligence has been received from or obtained about a client during the assessment of that client's legal situation or in the course of their duties of defending or representing the client in or concerning legal proceedings, including in the context of advice on how to initiate or avoid proceedings, whether such information or intelligence is received or obtained before, during or after such proceedings, unless the entities concerned have participated in money laundering or terrorist financing activities, have provided legal advice for the purposes of money laundering or terrorist financing, or know that the client has sought legal advice for such purposes.

The number of notifications received reflects, in some respects, the dynamic nature of the process and allows, to a certain extent, for the information to be updated. However, the authorities in charge of the register do not have the capacity to process all notifications received within a reasonable time frame, with the result that more than half of the notifications received between 2021 and early 2025 are still being processed, contributing to the continued presence of erroneous data in the register.

533. The competent authorities have access to information on beneficial owners which they request from FIs and, to a lesser extent, from DNFPBs. It should be noted, however, that reporting entities report substantial difficulties in identifying beneficial owners in cases involving complex chains of ownership involving foreign legal persons[156]. The authorities also use information available within the PCC, which has been set up to give them easier access to centralised information on the various accounts and financial contracts held by legal persons with financial institutions, and thus to trace the chain of persons acting as agents for accounts held by legal persons, who can also be identified as beneficial owners.

534. In conclusion, the competent authorities have timely access to information on beneficial owners via the UBO register. However, the mechanisms in place do not sufficiently ensure that the information is accurate. The absence of measures to check the accuracy of the information *ab initio* by the authority in charge of the register is a key issue which cannot be compensated for by the use of complementary mechanisms, such as notifications of discrepancies and targeted *ex post* checks. In this context, the UBO register is not a sufficiently reliable tool for the competent authorities to access accurate and current information on beneficial owners.

5.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information[157]

535. Belgian law does not authorise the creation of trusts or similar legal arrangements. It nevertheless requires foreign trustees and fiduciaries who meet certain conditions to register with Banque-Carrefour des Entreprises and to declare their beneficial owners, if they have not already been declared in another EU Member State, which is an improvement on the findings of the 2015 MER (see Rec. 25 TC Annex).

536. However, the Belgian authorities do not have sufficiently satisfactory information about foreign legal arrangements with a link to Belgium. There is no effective mechanism for systematically identifying foreign legal arrangements administered from Belgium. Access by the competent authorities to information held by the Cadastral Administration of SPF Finance makes it possible to identify trustees or fiduciaries who own real estate in Belgium. The information held by the tax authorities should make it possible to identify trustees, fiduciaries or beneficial owners linked to legal arrangements when they are resident in Belgium, but this information is not yet fully exploited for the purposes of identifying beneficial owners or ML/TF. At the end of January 2025, the tax authorities provided information on natural persons residing in Belgium who had declared themselves to be founders or beneficial owners of one or more trusts or similar foreign legal arrangements. This information is currently being analysed by SPF Finance to verify compliance with the requirements for registration in the UBO register.

537. Only 24 trusts and similar legal arrangements have been identified by SPF Finance as being required to provide information to the UBO register. Fourteen of these are in addition to the 732 trusts and similar legal structures that appear in the UBO register as intermediary entities of Belgian legal persons, but it has not yet been verified whether these entities also meet the definition of entities required to report

[156] Since 9 April 2024, Belgium has been connected to BORIS, the European platform providing access to the various national registers of beneficial owners. However, access at the Belgian level for entities subject to the legislation and the competent Belgian authorities is not yet operational. Foreign authorities in EU countries already connected to BORIS can consult data from the Belgian UBO register via BORIS.

[157] See the Methodology for Recommendation 25 regarding beneficial ownership information for legal arrangements.

information to the UBO register. In addition, more than 200 foreign entities registered in the Banque-Carrefour des Entreprises register are subject to supervision, as their names include words such as “trust” or “*fiducie*” without their legal form being known. Finally, external sources, such as the Panama Papers, are occasionally used to carry out additional checks.

538. Consequently, Belgium is unable to ensure that trusts and similar legal arrangements effectively fulfil their transparency obligations, in particular because it is unable to reliably identify the trusts and legal arrangements subject to these obligations if they do not declare themselves or are not identified by an obliged entity in the context of a business relationship. In this context, the Belgian authorities have limited access to accurate and up-to-date information on foreign legal arrangements. The limitations identified in section 5.3 also apply to foreign entities registered in the Banque-Carrefour des Entreprises and UBO registers concerning legal arrangements (see section 5.3).

5.5. Effectiveness, proportionality and dissuasiveness of sanctions

539. Belgium has administrative and criminal sanctions in place to punish breaches of obligations relating to the transparency of legal persons and entities, but these do not always appear to be dissuasive.

540. Criminal fines are applicable to legal persons who fail to comply with their obligations to register with Banque-Carrefour des Entreprises and to update certain data. However, these fines do not apply for data requiring the filing of a deed with the clerks of the commercial courts, which are subject to a specific regime governed by the CSA. For example, there are no administrative or criminal sanctions for failure to comply with the obligation to file the resignation of a director with the registry. In this case, only a civil sanction of unenforceability against third parties is possible, the effects of which do not appear to be sufficiently dissuasive in the context of frequent use of straw men. Between 2020 and 2024, the SPF Economy carried out an average of 9 074 annual checks on companies’ compliance with their obligations to report information to Banque-Carrefour des Entreprises. During this period, 1 492 reports were drawn up by the Directorate-General for Economic Inspection (DGIE) of the SPF Economy, which generally prefers to issue warnings and deregister incorrect data rather than impose sanctions. Deregistration is an administrative measure that has no impact on the legal existence of the company or its rights and obligations, but it can nevertheless hinder its administrative and economic activity (e.g. its relations with its bank, notary, accountant, etc.) and is therefore quite effective in this respect. It takes the form of a visible note on the Banque-Carrefour des Entreprises file of the entity concerned, which is removed as soon as the identified breaches have been remedied.

541. Failure to comply with the obligation to declare beneficial owners triggers the application of progressive measures (reminders as a preliminary formality prior to the application of an administrative fine), which generally appear to be proportionate and dissuasive. A one-year transitional period was granted to allow compliance following the introduction of the register in 2018. Regular reminder campaigns were carried out to encourage entities to voluntarily comply with this new obligation. Nearly 17 880 persons (26% of legal persons subject to reminder measures) received an administrative fine of EUR 250 or EUR 500 between July 2022 and June 2024, for a total amount of EUR 8.5 million, of which 75% has been collected. In addition, 55 703 legal persons were deregistered from Banque-Carrefour des Entreprises as a result of breaches of the obligations to register in the UBO register. Finally, in the event of failure to identify and communicate accurate and up-to-date information on beneficial owners, the directors of the legal person are liable to an administrative fine of between EUR 250 and EUR 50 000.

542. The Belgian authorities mainly use deregistration measures[158] and dissolution of "inactive" entities. These measures make it possible to target shelf companies and inactive non-profit organisations, whose frequent use has been clearly identified in ML/TF schemes. Around 10 000 non-profit organisations have been dissolved by the commercial courts of Hainaut and Liège as part of a project led by the SPF Economy (DGIE) aimed at dissolving dormant non-profit associations. The Brussels Commercial Court has dissolved 7 500 companies since 2018 as part of the "company dumping" project aimed at dissolving "ghost companies". Between 2014 and 2023, 336 judicial dissolutions were also ordered following inspections carried out as part of the BELFI project (see IO 9) in relation to the FT, mainly on the grounds of fictitious registered offices. Such dissolution measures are not provided for in the case of breaches of information obligations by active companies.

543. Failure to file annual accounts, which certain entities are required[159] to do for three consecutive financial years, has also led to the automatic deregistration of 23 028 entities from the Banque-Carrefour des Entreprises register.

544. Automatic deregistration for non-compliance with the obligation to submit information to the UBO register began in January 2024, with a total of more than 50 000 entities deregistered in January 2025, nearly 75% of which were non-profit associations. As with Banque-Carrefour des Entreprises, deregistration is an administrative measure that has no impact on the legal existence of the company or its rights and obligations, but which can hinder its administrative and economic activity and is therefore somewhat effective.[160]

[158] SPF Finance is authorised to request the automatic deregistration of entities that have not submitted the required information to the register and have not published any documents in the *Moniteur belge* for seven years, as well as those that have not registered information about their beneficial owners despite an administrative fine imposing the sanction for non-compliance. A third reason for deregistration is provided for but has not yet been implemented: failure to confirm data with the UBO register on an annual basis. The Belgian authorities estimate that this concerns more than 139,000 legal persons.

[159] Companies with limited liability, large non-profit associations and foundations are required to publish their accounts with the BNB. Small associations and foundations must file their annual accounts with the registry of the relevant commercial court. General partnerships and limited partnerships are only required to publish their annual accounts if certain criteria or thresholds are exceeded. Ordinary simple partnerships are entirely exempt from this obligation, as they have no legal personality.

[160] On the basis of the deregistration criteria related to non-compliance with UBO obligations, the failure to publish a deed in the *Moniteur belge* for seven years, and therefore the failure to update the basic information registered with Banque-Carrefour des Entreprises, also leads to automatic deregistration if the entity also fails to provide the required information on its beneficial owners.

6 Financial intelligence

The relevant Immediate Outcomes considered and assessed in this chapter is IO.6. The Recommendations relevant for the assessment of effectiveness under this chapter are R.29-32 and elements of R.1, 2, 4, 8, 9, 15, 34, and 40.[161]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) The CTIF has direct and indirect access to a large number of administrative and financial databases, which it actively uses to enhance its investigations. However, certain key information, such as virtual asset portfolios or virtual IBANs, is not yet collected in the central register of accounts and financial contracts (PCC) and, as a result, the CTIF does not have direct access to this information.

b) The CTIF is the source of financial intelligence produced to support investigations into ML, TF and predicate offences. It is frequently called upon to supplement the investigations carried out by competent authorities. The financial intelligence provided by the CTIF responds to the operational needs of the competent authorities, particularly in complex investigations involving organised crime, serious tax fraud and social security fraud. However, this information, like the financial information held by other competent authorities (in particular customs and tax authorities), is not used to its full potential by the authorities investigating and prosecuting ML. This raises concerns given the prevalence of laundering related to tax and social fraud, as well as the high risk associated with cash smuggling in Belgium. This underutilisation stems from limited analytical capacity, due to a lack of specialised resources, appropriate tools and technical expertise among investigative and prosecuting authorities. These constraints hinder the effective integration of financial intelligence into investigations and limit its use as a trigger for ML detection.

c) The CTIF has IT tools to carry out its operational and strategic analysis, but these remain limited given the growing volume and complexity of financial data. Until the end of September 2024, most STRs were processed via an electronic processing system that facilitated handling the increasing volume of reports. However, this tool had significant functional limitations, such as the lack of segmentation by risk type or predicate offence, and the inability to track transmission delays, which hindered the in-depth analysis of ML/TF typologies and the responsiveness of reporting entities. The deployment of the goAML system in October 2024 aims to address these shortcomings.

[161] Recommendations 1, 2, 3, 4, 8, 15, 34 and 40 are under review, see Technical Compliance Annex.

d) Despite the increase in the volume and quality of STRs, they mainly come from the financial sector, which limits the diversity of intelligence and hinders the detection of ML/TF typologies linked to low-reporting DNFBPs, particularly in at-risk sectors such as diamond traders, real estate and company service providers. Furthermore, reporting entities, particularly those with higher exposure or with low reporting levels, do not always receive sufficient, regular, or targeted feedback. This limits their ability to improve the quality, quantity and timeliness of STRs.

e) The CTIF produces in-depth, high-quality operational analysis that meet the needs of competent authorities. The predicate offences identified in the STRs and forwarded to the judicial authorities broadly correspond to Belgium's major risks. However, reporting entities tend to prioritise reporting the typologies highlighted by the CTIF (e.g., 'Brazilian' schemes), which may contribute to the predominance of certain patterns in STRs submissions.

f) The CTIF produces strategic analysis that are mainly typological in nature and useful for understanding risks and detecting emerging threats. However, their dissemination remains limited and some threats identified in national risk assessment (NRAs), such as terrorist financing and the ML through the real estate sector, are still insufficiently covered.

g) Belgium has put in place a number of mechanisms for exchanging financial intelligence on ML and TF, at both operational and strategic levels. Cooperation between all national authorities is close, effective and fluid, ensuring cooperation and exchange of information.

h) The judicial and law enforcement authorities integrate the financial aspect into account early in investigations, using all available information to locate proceeds derived from predicate offences. However, this approach remains focused on immediately available assets, and in-depth asset tracing investigations continue to be insufficient to fully uncover the proceeds associated with ML. This gap, which is more related to resource constraints and prioritisation than to the quality of financial intelligence, prevents the full identification of ML proceeds.

Recommended Actions

Belgium should:

a) Strengthen the financial intelligence capabilities of investigative agencies, in terms of human resources and specialised tools, to effectively support the use of financial intelligence, including that produced by customs and tax authorities, which must be systematically integrated into ML/TF investigations.

b) Equip the CTIF with advanced technological tools to analyse the increasing volumes of financial data and strengthen operational analysis capabilities.

c) Develop proactive strategic intelligence capabilities within the CTIF on emerging trends and new areas of ML/TF risk, and on managing and analysing the types of criminal activity detected, reporting delays, requests for information and communication between authorities.

d) Organise more frequent, regular and targeted feedback, both individual and sectoral, to reporting entities – particularly high risks and low-reporting sectors (such as diamond traders, real estate agents, company service providers/business centres, and lawyers) – and to supervisory authorities, covering the level of engagement, quality and timeliness of reporting, and how their reports are used.

e) Disseminate the strategic analyses prepared by the CTIF more widely, in a 'redacted' form where necessary, to raise awareness among competent authorities and reporting entities and foster a common understanding of the risks.

Overall Conclusions on IO.6

CTIF plays a central role in producing financial intelligence for combatting ML/TF, both operationally and strategically, and meets the operational needs of competent authorities to a large extent. It is frequently called upon to enrich investigations, drawing on a large volume of STRs and other relevant information, as well as its extensive access to various databases. However, the IT tools currently at its disposal are insufficient to process and make full use of the growing and increasingly complex volume of information that feeds into its operational and strategic analyses. Cooperation and sharing of financial information and intelligence between the competent authorities is otherwise close, fluid and constructive.

Nevertheless, the use of financial intelligence by investigative and prosecutorial authorities for ML purposes is not optimal. In particular, the information held by customs and tax authorities continues to be under-exploited, even though social security and tax fraud are among the main predicate offences identified in Belgium, and international cash smuggling is recognised as a major risk for the country. This underutilisation is due to the lack of appropriate analytical tools and technical expertise to deal with the increasing complexity of cases. These constraints hinder the optimal use of financial intelligence.

Moderate improvements are required.

Belgium is rated as having a Substantial level of effectiveness for IO.6.

Immediate Outcome 6

545. The evaluation team has based its conclusions on the cases presented by the authorities, the analysis of available statistical data and numerous interviews with the Belgian authorities and private sector representatives.

6.1. Timely access to relevant, accurate and up-to-date information

546. The CTIF has broad access to information essential for conducting its analysis, both through the reports it receives, mainly suspicious transaction reports (STRs),[162] and its access to several databases. Since 2022, the CTIF has been able to consult cross-border cash transport declarations directly via the Customs Information System (CIS) database.

6.1.1. Types of reports received

547. The CTIF plays a key role in receiving and analysing STRs from reporting entities, mainly in the financial sector (see table below). The volume of STRs received by the CTIF has been steadily increasing over the past five years (from 28,647 in 2020 to 89,457 in 2024). The nature and sophistication of these STRs vary considerably, particularly between sectors. Despite continuing sectoral disparities, this upward trend also reflects an improvement in the detection of suspicious transactions, as confirmed by the inspection reports of the AML/CFT supervisory authorities of reporting entities, particularly in the financial sector (see IO.3 and IO.4 on sectoral reporting activity).

[162] To a much lesser extent, reports sent by notaries and real estate agents when cash is used in real estate transactions in accordance with Article 66, §2 of the AML/CFT Law.

Table 6.1. Number of STRs received by the CTIF

	2020	2021	2022	2023	2024	
Financial institutions	26 893	41 403	49 019	75 304	87 902	Sharp increase – with notable rises in 2021 (+53.9%), 2023 (+53.6%) and 2024 (+16.8%)
DNFBPs	1 754	1 948	2 585	2 059	1 555	After an increase in 2022 (+31.6%), STRs fell in 2023 (-20.5%) and 2024 (-25.5%)
Total	**28 647**	**43 351**	**51 604**	**77363**	**89 457**	Overall growth – with significant increases in 2021 (+51.3%) and 2023 (+49.9%)

Source: CTIF

548. While the number of STRs has increased overall, sectoral disparities remain, with the majority of reports coming from FIs (96%), half from CIs (52% on average) and PIs. Conversely, some DNFBPs, despite being exposed to risks, some of which are significant, report very few suspicious transactions. This is particularly the case for diamond dealers, real estate agents, company service providers/business centres and lawyers, who remain under-represented in the reporting statistics (see IO.4). This high number of STRs from the financial sector, which reflects the overall importance of this sector, may have an impact on the diversity of financial intelligence available to the CTIF, thereby reducing its ability to detect certain types of ML/TF through non-financial channels.

549. Delays *in the transmission of STRs* by some reporting entities, in both the financial and non-financial sectors, is sometimes excessively long. For example, the inspections revealed cases where STRs were submitted more than three weeks after the end of the internal investigation, or even several months later. This situation raises concerns about the responsiveness and effectiveness of the reporting system for reporting entities, which could hinder early detection of certain ML/TF cases (see sections 3.4 of IO.3 and 4.4 of IO.4) and follow-up action.

550. To improve the *quality of STRs*, the CTIF is setting up a feedback system for reporting entities to improve their understanding of ML/TF typologies and refine their mechanisms for detecting suspicious transactions. This consists of talking directly with them, publishing guidance and holding awareness sessions (see section 6.3 for details on how this collaboration works and how effective it is). This feedback is having a positive impact, with noticeable improvements in how quickly reports are submitted and their quality. However, the feedback is still too limited to meet the needs of most reporting entities. It should be more frequent, especially for at-risk professions such as diamond traders and notaries.

551. The CTIF has also published an information note detailing the criteria for assessing the quality of STRs, which is a good way of improving the accuracy and relevance of the reports submitted by reporting entities. However, it has had limited real impact because the private sector has little or no knowledge of it. This suggests that these criteria need to be shared more widely.

552. Until very recently (end of September 2024), 95% of STRs were submitted electronically via the ORIS system, with reporting entities submitting their reports online using a secure form. This digitisation of the process made it easier to integrate reports into the CTIF database and helped to manage the growing volume of information received more efficiently. However, the ORIS system had several functional limitations, including the inability to segment reports, track reporting delays and analyse ML/TF trends. It was not possible to classify reports by type of risk or predicate offence, which prevented any detailed analysis of the ML/TF typologies reported. It was also unable to provide information on the time taken to submit STRs, which made it difficult to assess the responsiveness of reporting entities after detecting suspicious transactions.

553. Since 1 October 2024, the CTIF has been using the goAML reporting system. This tool, which some reporting entities, particularly small and medium-sized ones, still find difficult to use, includes advanced features for segmenting reports, tracking delays in reporting and analysing ML/TF trends. It aims to

optimise the use of STRs, improve how they are managed and strengthen the collection of statistical data on reporting activity.

6.1.2. Access to databases

554. The CTIF requests and obtains all relevant information from reporting entities, even if they have not submitted a report, and from the supervisory authorities or government agencies. To this end, it has signed memoranda of understanding (MOUs) with several partners, including the Belgian General Intelligence and Security Service (SGRS), the Belgian State Security Service (VSSE), the National Bank of Belgium (BNB), the Belgian Financial Services and Markets Authority (FSMA) and the European Anti-Fraud Office (OLAF). The CTIF also received information resources from other competent authorities (see table below), including supervisory authorities, and from its foreign counterparts (see IO.2).

Table 6.2. Information received from other competent authorities

	2020	2021	2022	2023	2024
Office for Advance Tax Rulings	604	489	413	298	710
SPF Finance (Anti-Fraud Co-ordination Service-CAF)	50	37	23	47	38
Customs & Excise [163]	1 076	632	117	42	12
SPF Economy	26	19	32	11	10
Europol		-	-	5	4
Trustees in bankruptcy and interim administrators	2	2	-	4	3
Security	16	9	5	3	4
Penitentiary institutions	1	-	2	3	3
Flemish Tax Service	36	32	8	2	1
General Intelligence and Security Service	2	4	2	2	2
Centre for Information and Advice on Sectarian Organisations	2	1	5	1	3
Coordination Unit for Threat Analysis (OCAM)	2	-	-	1	
Federal Prosecutor's Office	1				
SPF Foreign Affairs		-	2	-	
Social Inspectorate (federal and regional)	6	-	-	-	
Total	*1 824*	*1 225*	*609*	*419*	*790*

Source: CTIF

Table 6.3. Communications received from supervisory authorities and self-regulatory bodies

	2020	2021	2022	2023	2024
BNB	1				
FSMA	114	179	255	177	98
Institute for Tax Advisors & Accountants (ITAA)	3	57	253	79	31
SPF Economy – Licensing Unit (Diamonds)	12	5	11	-	4
National Chamber of Notaries		1	-	-	
Supervisory College of Auditors		-	-	-	2
Gaming Commission (CJH)	1				
Total	***131***	***242***	***519***	***256***	***135***

Source: CTIF

[163] The drop in the number of Customs STRs since 2022 is due to the fact that the CTIF can now access cross-border cash transport declarations directly via the Customs Information System (CIS) database, using an application developed by its ICC department.

555. The CTIF makes extensive use of the databases available to it in order to enhance its financial investigations. The National Register and Banque-Carrefour des Entreprises (see box below) are by far the most frequently consulted sources of information. However, other databases are also consulted on a regular basis. In 2024, for example, the CTIF made around 65,000 requests to the police database via its two liaison officers. Authorities regularly consult the central register of financial accounts and contracts (PCC) (4,208 times), as it gives them easier access to centralised information on various accounts and financial contracts, their holders and the financial institutions that maintain them. However, some data is not available, including virtual asset portfolios and virtual IBANs linked to main accounts. The Social Security databases (DOLSIS – SPF Social Security) were searched in 981 cases (usually with several searches per case) and the tax databases (SPF Finance) were searched to find information on 343 natural persons and 1,009 legal persons.

Box 6.1. Available files and databases (to which the CTIF has direct access)

To which the CTIF has direct access

- The *National Register* contains all identification data for the following natural persons: Belgians residing in Belgium; Belgian nationals residing abroad who are registered in the population registers kept by Belgian diplomatic missions or consular posts abroad; foreign nationals residing in Belgium who are admitted or authorised to settle or reside in Belgium, and foreign nationals who declare themselves refugees or who apply for refugee status.
- The *Banque-Carrefour des Entreprises* contains all identification data for the following entities: legal persons under Belgian law; natural persons who are self-employed in Belgium; legal persons under foreign law with a head office or branch in Belgium; organisations without legal personality that, in Belgium, are either a company, subject to social security as an employer, or subject to VAT; bodies or agencies governed by Belgian law that perform public service remits or remits related to public order and have financial and accounting autonomy separate from that of the legal persons governed by Belgian public law to which they are attached; natural persons or legal persons governed by foreign law and organisations without legal personality required to register under specific Belgian legislation.
- *Social security and employment databases*: via the DOLSIS application, including employment declarations, employer and employee files, pension and unemployment data.
- *Central criminal records system*: lists final convictions of natural persons and legal persons (complete for legal persons since 2016).
- *Tax databases*: tax returns (personal income tax, corporation tax, VAT), customer/supplier lists and cadastral data.
- *UBO register*: centralises information on the ultimate beneficial owners of Belgian companies and legal persons.
- *Centralised register* of financial accounts and contracts held by legal persons with Belgian financial institutions (PCC): established in 2011 for tax purposes and access extended for ML purposes in 2018. Register managed by the National Bank of Belgium's central point of contact.
- *Banque de données communes* (BDC): information on terrorism, extremism and radicalisation (restricted access). See IO.9.
- *Customs and financial systems*: CIS (Customs Information System) via AFIS and the CIS (Customs Information System) database. Since 2022, the CTIF has also had direct access to cross-border cash transport declarations via the European Commission's Customs Information System (CIS) database, thanks to a dedicated application developed in-house by its ICC department.

- *Centrale des Bilans*: compiles the annual accounts of Belgian companies filed with the National Bank of Belgium.

To which the CTIF has indirect access

- *KIK police database*: can be accessed daily by the federal police liaison officer, with a standard response time of 24 hours and an emergency procedure that can be initiated every 15 minutes for urgent requests.
- *Public Prosecutor's Office* ADBA database: contains information supplementing the police databases, accessible by the CTIF via the federal police liaison officer, with a response within one to two days.

556. While the databases used by the CTIF and other authorities, such as the Banque-Carrefour des Entreprises, are generally considered useful sources of information, concerns have been raised about the updating and completeness of the basic data held by the Banque-Carrefour des Entreprises and about the beneficial owners listed in the UBO register (see IO.5). These shortcomings limit the authorities' ability to make full use of these databases, which in turn may reduce the scope and reliability of the financial intelligence generated, thereby affecting the effectiveness of ML/FT investigations (see IO.7).

557. Investigative authorities also have broad access to various databases that are essential to their ML/TF investigations and to locating the proceeds of crime, and which serve as sources for enhancing financial intelligence. In practice, the Federal Judicial Police play a key role in using this data, carrying out searches and reporting their findings. At the same time, with a judge's written authorisation, the investigative authorities can obtain all relevant information from other national authorities within a response time of between 24 hours and five working days, which can slow down certain procedures. Furthermore, when investigating social security and tax fraud, the police and prosecutor's offices can draw on the expertise and operational support of finance officials and social security inspectors as part of multidisciplinary investigation teams (MOTEMs). In practice, the use of MOTEMs is limited and has not yet delivered tangible results in ML investigations (see IO.7).

558. For their part, prosecution authorities generally have similar access to information as the police, thereby ensuring continuity in the analysis and processing of cases.

6.2. Production and dissemination of financial intelligence

559. In 2024, the CTIF received around 91,000 STRs. Of these, around 15,000 were processed by the ML/TF department. To cope with this volume, the CTIF has implemented a multi-step process, consisting of initial screening, triage and enhancement, followed by in-depth analysis.

560. Until recently, this work was largely done manually. Enhancing STRs took analysts about two days per report before they could be added to the analysis pipeline. This way of working had obvious limits in terms of efficiency and responsiveness. Since early October 2024, STRs have been managed through the goAML system, which supports predefined indicators and structural elements, paving the way for more automated processing. The goal is to improve detection and prioritisation of urgent cases, while ensuring faster, more targeted analysis. As goAML has only recently been implemented, no conclusions can yet be drawn about how efficiently reports submitted to the CTIF are being processed.

561. The Triage and Enhancement Department, made up of seven to eight administrative staff, plays a key role in the initial screening of STRs. It carries out this screening using a set of objective criteria to identify the most critical reports. This preliminary analysis routes STRs to the relevant department for in-depth processing or, in less complex cases, for rapid analysis within the Triage team itself.

562. This work involves several tools and databases, including the CTIF's internal databases, to search for possible matches with existing cases; police databases, accessed through the two liaison officers seconded to the CTIF; and the FIU-Net network, to identify any links with financial investigations conducted by other financial intelligence units (FIUs) abroad.

563. A scoring system is used to classify STRs according to their priority level (by type, e.g. ML, TF, tax offences) in order to streamline how they are handled. The evaluation team reviewed the internal procedures and scoring system and found them to be appropriate and relevant. STRs requiring only a quick analysis are handled directly by the Triage and Enhancement Department, which then forwards them to the most relevant authority. This department is also responsible for sending financial intelligence to foreign FIUs via FIU-Net, through the XBD and XBR processes (see IO.2).

564. Lastly, requests for information and spontaneous communications received from foreign FIUs are handled in the same way as domestic STRs, thereby ensuring consistency in how financial intelligence is analysed and disseminated (see IO.2).

6.2.1. Production of financial intelligence

565. The CTIF's analysis and dissemination activities largely support the competent authorities' operational needs. The competent authorities interviewed during the on-site visit confirmed their close cooperation with the CTIF, its ability to disseminate high-quality reports and their suitability for operational requirements in connection with ML investigations and prosecutions, predicate offences and TF. Belgium provided a number of case studies confirming this.

Operational analysis

566. The CTIF plays a key role in producing financial intelligence, conducting in-depth operational analyses which it disseminates proactively or on request to the competent national authorities and its foreign counterparts. Its ML/TF department, comprising 20 analysts, including two dedicated to TF analysis, is responsible for the operational processing of STRs. This is considered to be sufficient in terms of capacity. Among the 18 generalists, some have specialisations in virtual assets, the diamond sector or tax fraud.

567. The CTIF handles files at a steady pace, with an average of 100 to 200 files per analyst (depending on their level of experience). Approximately one file is handled per analyst per day, but the analysis work involves managing several files at the same time and can be slowed down by time delays in receiving responses from external sources. The average time taken by the CTIF to process suspicious transaction reports is approximately three months. However, some files, particularly those considered urgent, can be processed within a few days to a few weeks. These processing times reflect the complexity of the analysis and enhancement work carried out by the CTIF to produce actionable financial intelligence. It should be noted that these statistics are influenced by certain exceptional cases, such as a file opened in 2015, which remained formally open for 2 659 days due to the wait for external triggers, before finally being forwarded in 2023 following a request received nine days before dissemination.

568. The CTIF has adopted a priority-based approach to optimise the processing of files. This process is based on the targeted selection of STRs according to risk criteria, enabling certain categories of files to be processed more quickly. For example, around 2021, STRs related to the Sky ECC case (see IO.7) were dealt with as a priority. Similarly, STRs relating to Brazilian networks involving offsetting schemes were dealt with proactively, with a view to reducing the number of spontaneous communications.

569. Screened STRs are not automatically subject to in-depth operational analysis, but they are fed into a database that provides essential information to support future investigations. The aim of this approach is to quickly identify STRs that have the greatest potential for investigation, while reducing the workload of analysts and ensuring more efficient use of resources.

570. The processing of urgent files varies greatly depending on the severity and the steps required. Thanks to its direct access to databases and inter-agency cooperation, the CTIF can quickly obtain the information needed to process certain complex files within a day if necessary. The CTIF also has the right to block suspicious transactions and has a five-day window to do so, which has been found to be enough time to analyse the situation and prepare any information to be sent to the judicial authorities (see IO.8).

571. The CTIF makes use of several tools to ensure that its analysts adopt an effective and consistent approach to their work:

- Internal procedure notes defining investigation methods, database searches, information gathering from reporting entities and authorities, and file management and forwarding.
- An STR scoring system that prioritises STRs based on the risk inherent in each case and directs resources to the most critical cases.
- A summary of reporting obligations specifying the information that must be provided to the various competent authorities.
- An international cooperation matrix for managing communications with foreign FIUs while protecting personal data.
- Internal training for analysts, including monthly newsletters, RADAR notes and workshops provided by other institutions.

572. Operational analysis relies on close interaction with other departments within the CTIF, particularly the Triage and Enhancement Department and the Strategic Analysis Department, which are part of the same division. This collaboration facilitates the sharing of information and optimises the quality of investigations.

573. The CTIF has IT tools to carry out its operational analyses, but their use remains limited given the increasing volume and complexity of financial data. The lack of advanced technological tools, such as specialised software, data mining or automated analysis solutions, makes it difficult to manage information flows effectively and undermines the analysis of financial flows, data traceability and the strategic use of data.

Strategic analysis

574. The Analysis department, comprising four analysts, produces in-depth strategic analyses to identify emerging trends. Drawing on the 2023 Money Laundering National Risk Analysis (ML NRA), international trends (observed by FATF, Europol, foreign FIUs), national developments and internal information, such as that from operational analysis, this department develops targeted strategic analyses that enhance authorities' response capabilities.

575. Since 2019, the CTIF has produced 12 strategic analyses targeting criminal threats, money laundering techniques and at-risk sectors and countries. This work has identified patterns linked to drug trafficking, organised crime groups and fraud, as well as sophisticated methods such as money laundering through the Brazilian network, the abuse of corporate vehicles and underground banking. This analytical approach is broadly in line with Belgium's risk profile, as outlined in the ML NRA, which highlights in particular the predominance of cash, the role of professional money launderers, fictitious legal structures and investment in real estate (see IO.1). Some analyses, regularly updated through to 2024, adopt a cross-cutting approach, drawing on both lessons learned from operational analysis and broader strategic insights. For example, the 2024 analysis on ML linked to cyber-enabled fraud is based on a growing number of STRs received by the CTIF, while placing these findings in the context of trends identified at the international level (FATF and Europol). In another note from 2020, focused on Brazilian networks, the analysis highlights a money laundering scheme involving multiple criminal offences, with a combination of several predicate offences such as serious social security and tax fraud, human trafficking, drug trafficking and fraud, often linked to cyber fraud. The published note includes typical money laundering patterns (red

flags), a detailed description of credit/debit transactions and an analysis of financial flows, particularly to Asia.

Box 6.2. Alignment of the CTIF's strategic analyses with the main national threats, in particular

- Money laundering from drug trafficking: regularly identified as a national priority, this is covered in detail in the analyses (2019, 2023).
- Professional money launderers and structured networks: addressed through studies on professional money launderers (2024), the Brazilian network (2022) and underground banking (2023).
- Abusive corporate vehicles and tax/social security fraud: adequately addressed through analyses on the abuse of structures (2022) and the creation of shell or sham companies.
- Fraud and cyber fraud: an emerging issue that is addressed in detail in the 2024 analysis.
- Organised crime groups (OCGs): analyses focusing on Italian, Albanian and Chinese OCGs demonstrate a targeted approach based on origin or criminal community.
- At-risk countries and sectors: Dubai, gambling and, to a certain extent, diamonds are covered.
- Cross-border cash movements through Belgian airports (2024).

576. Although the CTIF's strategic analyses cover several of the risks identified in the ML and TF NRAs, a number of key threats are still only partially covered or not covered at all in these analyses. The widespread use of cash, although addressed in several strategic analyses, is not dealt with in a cross-cutting manner, particularly in relation to cash-intensive sectors. No dedicated analysis has yet been undertaken on virtual assets, despite their growing role in ML/TF typologies (see IO.7 and IO.9). Similarly, fictitious legal arrangements, shell companies and sham entities, although addressed in the analysis on the misuse of corporate vehicles (2022), could be examined in greater depth, particularly with regard to the use of straw men, which is prevalent in the majority of ML cases. No distinct strategic analysis appears to have been conducted on real estate, despite it being identified as an at-risk sector for ML. Furthermore, emerging risks associated with the use of virtual IBANs and new financial services (fintech, neobanks) have not been explored in depth. Lastly, the TF perspective is largely absent from strategic analyses, even though the 2023 TF NRA highlights specific threats related to microfinance, the use of small amounts of cash and new payment methods.

577. All of these strategic analyses are shared internally with CTIF staff. However, only four have been forwarded to the competent authorities, which limits their operational scope. These strategic analyses are nevertheless essential tools for understanding risks, raising awareness among relevant stakeholders and alerting them to emerging threats. At present, their dissemination is still too limited, particularly among the reporting entities, which hampers the early detection of money laundering patterns and reduces authorities' responsiveness. The lack of proactive dissemination, even with redacted versions tailoring the content to different audiences, limits their practical impact on raising awareness among relevant stakeholders.

578. The CTIF develops other high-quality strategic output for internal distribution, such as analysis notes, information notes, analysis sheets and a biannual strategic bulletin called 'RADAR' focusing on established trends, risk areas and early warning signs. This document has been shared with the Strategic Analysis department of the Federal Judicial Police.

579. The CTIF's publication of annual reports, typological analyses and practical guides for reporting entities (Vademecum) provides reporting entities, competent authorities and other stakeholders with key

tools to improve their understanding of the risks and adjust their mechanisms for detecting suspicious transactions. However, given the low level of implementation of AML/CFT obligations and the sometimes limited understanding that some reporting entities have of the risks, the visibility and effective use of these documents are still major challenges. More targeted dissemination and monitoring of their impact are needed to maximise their usefulness and improve the effectiveness of ML/TF measures.

580. The Intelligence Coordination Centre (comprising two data analysts) has implemented tools to support operational and strategic analysis. However, these tools do not include advanced technological solutions (such as analysis software, data mining solutions, etc.) that can process large volumes of data efficiently. This limits the in-depth use of CTIF data, particularly for proactive strategic analysis aimed at detecting and anticipating new trends or types of ML/TF.

581. Although the implementation of the goAML system at the end of 2024 is expected to improve the management of incoming information (classification of STRs, data structuring, timeliness of STRs, etc.) and make it easier to provide feedback to reporting entities and supervisory authorities, this tool still does not allow the available data to be used to its full potential, particularly for operational and strategic analysis purposes.

6.2.2. Dissemination of financial intelligence

582. When an analysis uncovers serious signs of ML/TF, the CTIF forwards its findings to the judicial authorities (district or federal prosecutor). However, the AML Law does not allow the CTIF to share this information directly with the police. In human trafficking or social security fraud cases, a copy is also sent to the labour prosecution service (which specialises in social security fraud). In 2024, the CTIF forwarded 3,054 files (new files and additional information) to the judicial authorities, working with a team of approximately 25 full-time-equivalent analysts and administrative staff, equating to an average of 122 files forwarded per analyst over the year. This volume is considered satisfactory given the resources available.

583. Between 2020 and 2024, the CTIF forwarded 6,389 new cases to the judicial authorities, involving an estimated total of €9.98 billion in illegal proceeds. At the same time, 8 131 pieces of additional information were provided to supplement cases already in progress, involving an additional €1.61 billion. Over this five-year period, the judicial authorities therefore benefited from information from 14,520 STRs, for a combined total of €11.58 billion. In addition, in 2,105 cases, a copy of the file was also sent to the labour prosecution service, particularly where the cases concerned offences related to social security fraud or human trafficking. However, a significant proportion of these referrals do not result in an investigation being opened, owing to a lack of sufficient resources available to the judicial authorities (see IO.7).

584. Furthermore, the CTIF shares and communicates information with the various services/authorities listed below:

Table 6.4. Communication by the CTIF (based on Art. 83 of the AML/CFT Law)

	2020	2021	2022	2023	2024	Total
SPF Finance (Anti-Fraud Co-ordination Service - CAF)	271	268	363	675	683	2260
Customs & Excise	10	35	15	23	13	96
SPF Social Security (SIRS)	251	242	368	583	471	1915
SPF Economy (for investigation)	24	17	4	20	15	80
FSMA (for investigation)	-	-	2	6	9	17
OCSC	39	50	56	68	110	323
Coordination Unit for Threat Analysis (OCAM)	142	97	85	51	35	410
State Security (VSSE)	142	97	85	51	35	410
General Intelligence and Army Security Service (SGRS)	142	97	85	51	35	410
Banque de données communes (BDC)	31	8	30	11	13	93
General Treasury Department	-	-	-	4	3	7
OLAF	-	-	-	3	1	4

585. In addition, the CTIF continues to cooperate actively with the three AML/CFT supervisory authorities – mainly the BNB, the FSMA and SPF Economy – by exchanging information on, among other things, the reporting activities of reporting entities, any AML/CFT non-compliance identified during the operational analysis of files, the results of individual risk analyses or inspections carried out by supervisory authorities, their respective expertise on specific topics, and reports following referral to the prosecutor's office of cases involving reporting entities. This exchange of information is evidence of ongoing inter-institutional cooperation, which helps to strengthen the supervisory chain.

Table 6.5. Exchange of information between the CTIF and supervisory authorities

	2020	2021	2022	2023	2024	Total
BNB	13	21	21	17	18	90
FSMA	3	6	13	8	5	35
SPF Economy	28	14	15	38	30	125
SPF Finance (Bpost)	1	1	1	1	0	4
National Chamber of Notaries	2	1	4	3	10	11
Institute for Tax Advisors & Accountants (ITAA)	2	7	9	1	7	26
Supervisory Board of Company Auditors	1	0	3	4	2	10
Bar Associations	0	1	1	6	4	12
Gaming Commission	2	2	0	2	2	8

Box 6.3. Example illustrating the relevance of CTIF communications

i. **To the FSMA in guiding its supervisory activities**

Exchanges between the CTIF and the FSMA led in 2023 to a thematic supervisory action targeting the reporting activities of bureaux de change. This initiative came in response to observations made by the CTIF, shared at a regular meeting, concerning an abnormal concentration of STRs from one operator in 2022, a significant decrease in STRs from others, and a level of quality deemed insufficient across the sector as a whole. The supervisory action was subsequently incorporated into the on-site inspections carried out by the FSMA.

ii. **For more targeted supervision by SPF Economy**

Between 2021 and 2023, these exchanges led to 17 files being opened, six of which resulted in reports, relating in particular to diamond traders, company service providers (business centres) and cash payments. This was done when a report was also forwarded to the prosecutor's office. The data provided by the CTIF enabled SPF Economy to target reporting entities more effectively, as well as the 'client' files for analysis, particularly in the company service providers sector.

iii. **In the notarial sector**

In 2022, two notarial firms were reported for alleged non-compliance with AML/CFT obligations in similar situations involving the formation of at-risk companies (susceptible sectors, foreign founders, business introducers, shared addresses). These reports were referred to the executive committee of the National Chamber of Notaries, which initiated administrative sanction proceedings for failure to comply with the obligations of the AML Law. One of the two cases resulted in an administrative fine for non-compliance with the ban on disclosure and failure to report suspicious transactions. The other case was dismissed.

6.2.3. FIU financial intelligence supporting needs of competent authorities

586. The financial intelligence provided by the CTIF is tailored to the operational needs of the competent authorities, particularly in complex investigations involving organised crime, serious tax fraud and social security fraud. Over the years, the forwarded files have helped to document the interconnected nature of these predicate offences, highlighting examples of money laundering involving multiple criminal offences (such as the Brazilian networks). These referrals regularly reveal criminal structures that use sophisticated financial offsetting techniques, which are characteristic of organised networks. This type of information, which is only available to the CTIF, provides the judicial and law enforcement authorities with critical added value by helping them to understand financial flows, identify beneficial owners and strengthen financial evidence in investigations.

587. Feedback has been generally positive, with prosecutors, investigating judges and police services highlighting the quality and relevance of CTIF analyses, which are disseminated both proactively and on request, thereby helping to open new investigations and strengthen ongoing ones. See below for practical examples of the use of financial intelligence, particularly in cases involving high ML risks.

Box 6.4. Example illustrating how CTIF financial intelligence meets the needs of competent authorities through a Trade-Based Money Laundering (TBML) typology

Between 2022 and 2024, the CTIF submitted several files documenting international trade-based money laundering (TBML) schemes combined with offsetting mechanisms. In these cases, Belgian companies active in the construction sector made payments to wholesalers located in Asia or the EU for the purchase of goods that were actually intended for retail companies linked to criminal networks. These trade flows were used to recycle the proceeds of illegal activities, particularly drug trafficking. The goods involved ranged from everyday consumer goods (e.g. textiles imported from China) to luxury goods (e.g. watches and top-of-the-range vehicles). These files also revealed associated customs fraud, such as undervaluation.

Outcome: This type of financial intelligence has provided critical added value to competent authorities to help them understand the economic structures used and target the entities involved.

Box 6.5. Example illustrating the role of CTIF in the early detection and classification of 'Brazilian' networks'

'Brazilian' networks, characterised by the use of short-lived companies in the construction and industrial cleaning sectors, often involve Portuguese or Brazilian nationals. Through analysis of DOS reports received, CTIF has documented the evolution of these structures towards increasingly complex arrangements, combining social fraud, undeclared work and money laundering.

Results: These observations have raised awareness among judicial authorities of the growing seriousness of the phenomenon and its economic impact, directing their attention towards structured networks of shell companies operating according to repetitive patterns.

588. Since 2017, the number of TF-related STRs has been steadily falling, a trend linked to the shift towards microfinance models, which are more difficult to detect (see IO.1 and IO.9). Despite this challenge, the CTIF has played a key role, recognised by the competent authorities, in detecting TF-related networks. For example, the Syrian Wallets project has led to many TF cases being opened (see box in section 9.1 of IO.9).

589. In terms of ML, a significant proportion of the files forwarded by the CTIF are not used to their full potential. Between 2019 and 2024, 43% of files forwarded by the CTIF to the judicial authorities were closed without further action ('no criminal prosecution'). This situation is primarily due to the lack of resources available to the police and, as far as can be determined, not to the quality of the information provided by the CTIF (see IO.7).

6.2.4. Other competent authorities producing financial intelligence (where relevant)

590. In cases of serious tax fraud, whether organised or not, cooperation between the CTIF and SPF Finance's Anti-Fraud Co-ordination Service (CAF) provides valuable additional support to the CAF's anti-tax fraud procedures. The CTIF regularly sends relevant information to the CAF, at the same time as it sends files to the judicial authorities. All files forwarded by the CTIF are entered into the StrirFraude application

of the Special Tax Inspectorate (ISI), where they trigger preliminary investigations and, if necessary, tax investigations. The significant increase in referrals from the CTIF to the CAF (from 268 in 2021 to 683 in 2024) reflects the ongoing improvement in the exchange of information and the development of financial intelligence by other competent authorities, in particular by incorporating the CTIF's analyses. Furthermore, if the CAF detects any signs of ML while carrying out its work, it informs the CTIF (see table 6.1).

591. In cases of suspected serious tax fraud, the tax authorities refer the matter to the relevant prosecutor's office, which decides whether it should be dealt with through criminal or administrative tax proceedings. These files involve complex fraud schemes, including the use of offshore structures or fraudulent structures in the diamond sector. The tax authorities refer around 150 files involving serious tax fraud, whether organised or not, to the judicial authorities each year. However, these cases do not necessarily result in money laundering investigations relating to aggravated tax fraud, and the judicial authorities therefore do not make full use of the financial information available to the tax authorities in ML cases. The proportion of ML cases linked to tax fraud referred to prosecutor's offices between 2019 and 2023 was 4%, which seems low given that tax fraud is identified as one of the most prevalent ML offences (see IO.7).

592. Customs authorities collect information on declarations of cross-border movements of cash and bearer negotiable instruments (BNIs). When a customs offence is detected, a report is sent to the prosecutor's office. They also send reports to the prosecutor's office when no offence has been detected but there is suspicion of criminal activity. The CTIF has access to this data via the Customs Information System (CIS) database and uses it mainly for strategic analysis purposes. The information available may include identity, circumstances, sometimes a hearing or photos, indications or suspicions of ML/TF, and other information from customs databases. In addition, customs authorities also respond to requests for information received from the CTIF. However, this customs information is not used to its full potential by the authorities responsible for investigating and prosecuting ML. The number of reports forwarded by customs to the judicial authorities remains relatively low. Between 2019 and October 2024, 149 reports/records were forwarded following inspections carried out at Brussels-Zaventem and Charleroi international airports (see IO.8). Given the prevalence of cash in ML/TF cases, this underutilisation of customs information by the judicial authorities is a significant shortcoming.

6.3. Cooperation and exchange of information/financial intelligence

6.3.1. Co-operation and exchange

593. Cooperation between national authorities ensures that financial intelligence is shared efficiently. The CTIF plays a key role in this process by coordinating the sharing of information and contributing to strategic initiatives such as the development of NRAs (see IO.1). This collaboration extends to joint projects such as BELFI[164] (see IO.10) and the strategic counter-terrorism meetings (MONITOR) (see IO.9), which facilitate consultation between the CTIF and other competent authorities, both at an operational level and in the sharing of intelligence.

594. A well-established system of cooperation also exists with the federal police, through a police liaison officer (DGJ-DJSOC[165]) seconded to the CTIF and through regular interaction with several specialised services, particularly in matters relating to drugs, corruption and organised crime. In practical terms, the use of this liaison officer has allowed the CTIF to broaden the scope of its operational analysis. In one case,

[164] The BELFI project is a multidisciplinary project to combat fraud (tax, social security, financial, etc.) through closer collaboration between judicial, tax and administrative authorities.

[165] Judicial Police Directorate-General – Directorate for the Fight against Serious and Organised Crime

for example, the officer helped the CTIF identify suspicious financial transactions abroad, enabling it to target its requests to a foreign FIU.

595. Close cooperation has been established between the CTIF and the police to make it easier to share strategic information, even though there are legal limits on sharing operational analysis directly. For example, the DGJ-DJSOC asked the CTIF to help map Italian mafia organisations in Belgium. As part of this effort, it put in place a special procedure and added an 'Italian MAFIA' file to its database, strengthening the analysis of financial flows linked to these criminal networks. This coordinated approach between the CTIF, the judicial authorities and specialised services is an example of effective action against the financial and criminal threats Belgium faces.

596. The CTIF also collaborates with the VSSE, SGRS and OCAM in combating terrorism and TF. In 2023, the CTIF shared 51 files with OCAM's intelligence services, and over the last three years, this figure stood at 233 files, illustrating how important it is to share information under the AML/CFT framework. Since 2021, the CTIF has also been participating as a partner service in the Terrorism, Extremism and Radicalism (TER) Strategy (see IO.9). The CTIF has access to OCAM's shared database (see IO.9), enabling it to check whether certain entities are listed there. Over the last five years, it has carried out 205 searches to supplement its files. It can also add relevant information and has contributed to 126 files over the same period.

597. Since early 2022, the CTIF has been working with the judicial authorities and SPF Finance on a project to crack down on shell companies used by networks known as 'Brazilian networks', which are involved in various criminal activities, such as social security fraud, drug trafficking, scams and arms trafficking. These criminal networks operate using a particularly complex and constantly evolving model. They create, in a very short space of time, multiple shell companies designed to channel large flows of illegal funds without being detected by the authorities. To address this challenge, the CTIF has set up a specific alert mechanism, in the form of a 'FB – Urgent Block' report, which is systematically forwarded to the relevant prosecutor's office so that it can take swift action.

598. However, the impact of this initiative is more significant for tax purposes than for money laundering, as it enables the recovery of tax debts based on the amounts seized and then transferred to the OCSC. In judicial terms, this initiative has led to the dismantling of criminal structures and the recovery of funds from the predicate offences. However, the focus is on tax fraud and recovery, with no consideration given to ML aspects. This approach demonstrates the importance of cooperation between the CTIF, the judicial authorities and the tax authorities in tax matters, which are not, however, being fully leveraged to maximise the impact of financial investigations and strengthen actions to combat ML.

599. The CTIF also works closely with supervisory authorities to support them in carrying out their duties. Its communications with these authorities fall into three main categories: feedback on the reporting activity of reporting entities (quantity and quality of STRs submitted), reporting of non-compliance with the obligations under the AML/CFT Law, and provision of specific information related to legal cases involving entities under their supervision. This cooperation helps to strengthen the effectiveness of supervision and improve compliance with AML/CFT obligations in the financial and non-financial sectors. See the subsection on the *Dissemination of financial intelligence.*

600. In addition, the CTIF attends, as an observer, the AML/CFT colleges of supervisors regularly organised by the BNB for Belgian financial institutions under its supervision that have subsidiaries, branches or other forms of establishments in at least two other EU Member States. The CTIF frequently prepares feedback on the reporting activity of the supervised member of the college. Furthermore, each year, the CTIF submits a report on the reporting activity of Bpost to the SPF Finance Treasury Administration.

601. The CTIF maintains close and effective cooperation with Belgian prosecutors from the European Public Prosecutor's Office (EPPO). A significant proportion of the case files handled by the EPPO are based on reports made by the CTIF, and the financial intelligence provided on request is considered to be of high

quality. Working relations between the CTIF and the Belgian national prosecutor's office are also smooth and constructive. The CTIF also cooperates with Europol within the framework of Europol's public-private financial intelligence partnership.

Box 6.6. Example of good cooperation between the CTIF and the EPPO

Facts: As part of an investigation into correspondent banking operations, the EPPO requested assistance from the CTIF. The searches identified several matches in the database. After targeted discussions on the EPPO's needs, a second request was made with additional details.

Outcome: This collaborative effort resulted in the CTIF forwarding two files. The information provided added value to the investigation by identifying new operators, banking transactions transiting through Belgium and suspicious structures, thereby helping to broaden the scope of the investigation into a complex money laundering case.

6.3.2. Security and confidentiality

602. The CTIF applies strict technical and regulatory measures to guarantee that information is kept confidential. Access to its premises and systems is restricted, and security protocols are in place governing the use of databases, IT resources and documentation. Communications with other relevant organisations are routed through secure channels.

603. The CTIF has signed several memoranda of understanding (MOUs) with national authorities (e.g. BNB, FSMA) defining the procedures for exchanging information using secure systems. Information is forwarded to the intelligence services by a VSSE liaison officer, while information forwarded to the judicial authorities is still largely sent by unsecured means, by post or registered mail, depending on the prosecutor's office.

604. At the international level, information exchanged with foreign counterparts is secured via FIU.NET and Egmont Secure Web.

6.4. Use of financial information/intelligence

6.4.1. Use of financial information/intelligence for investigations and developing evidence

605. In general, the investigative and prosecuting authorities incorporate financial intelligence provided by CTIF into their investigations, in addition to other sources of information. This data is essential for gathering evidence, locating the proceeds of crime and understanding financial flows linked to ML, TF and predicate offences. The combined use of sources from the CTIF, national databases, conventional investigative techniques (searches, phone tapping and surveillance) and specialised resources (virtual asset tracing, decryption) strengthens case files and broadens the scope of investigations. However, other sources of financial intelligence (e.g. from CAF and Customs) are not used to their full potential in ML investigations. Financial intelligence from CTIF has helped identify new players, establish operational links and substantiate charges. The examples in section 6.2 demonstrate this added value in complex cases such as those involving shell company structures, suspicious flows in offsetting and TBML schemes, or to support investigations conducted by the various federal judicial police units nationally and partners such as the EPPO.

Box 6.7. Role of the CTIF in the Sky ECC case (Limit and Edge Operations)

Facts: In March 2021, the press revealed that SKY ECC, an encrypted communication system used by criminal networks, had been hacked. Two major judicial investigations followed: Operation Limit, targeting the service provider, and Operation Edge, targeting the criminal organisations identified by the DGJ-DJSOC.

CTIF role: Since July-August 2021, the CTIF has been actively collaborating with the Edge unit, the Antwerp federal judicial police unit and the Federal Judicial Police Directorate-General to coordinate the financial analysis. It received lists of identified users from August 2021 to June 2024. The CTIF adds its own data (files transmitted, known entities) to this database and makes additional requests (ref. Art. 80 of the AML/CFT Law).

Results: The CTIF adds strategic value to investigations by identifying links between SKY ECC users and its own ML files. It helps prioritise cases according to the seriousness of the offence and supplements the police's Edge database. This facilitates coordinated processing and effective information sharing. This collaboration strengthens the judicial and financial investigation of a very large, organised crime case in Belgium.

606. From this perspective, the CTIF is a key support for BC investigations, especially as a regular point of contact for the specialised units of the Federal Judicial Police Directorate-General (DGJ). The DGJ liaison officer seconded to the CTIF can, at the request of the judicial authorities, check whether the CTIF has information on the natural and/or legal persons targeted by the investigation and, if so, supplement the investigation with additional financial intelligence, including using the option of requesting information from foreign FIUs. The CTIF cannot make use of this option if it does not already have related information based on the STRs received and its analyses. This condition limits rapid access to certain information that is useful for strengthening international investigations, particularly when urgent action is required (see IO.7 and IO.2). The judicial authorities can also send information directly to the CTIF and highlight the high quality of the information provided in response. This information is regularly used by law enforcement agencies to support and strengthen ongoing investigations or initiate new ones. It provides valuable insight into suspicious financial flows, connections between actors and complex structures, thereby strengthening the case for prosecution. Although the judicial authorities have not provided detailed statistics on the requests made to the CTIF, case studies demonstrate that this information is frequently used and provides real added value in terms of evidence, traceability of criminal flows and identification of ML structures (see IO.7).

607. Belgium also provided examples demonstrating how financial intelligence generated by the CTIF was used by judicial authorities and the police in TF investigations (see IO.9).

608. However, this effectiveness is hampered by certain organisational constraints. The increasing complexity of ML/TF cases often requires the use of new analytical tools, particularly when dealing with transnational structures or the use of virtual assets. While judicial authorities praise the quality of investigators' work and the information they produce, they also point to a lack of police resources, both human and in terms of equipment and IT. The shortage of investigators trained in financial matters, cybercrime and the traceability of crypto-assets prevents financial intelligence from being used to its full potential. Similarly, the IT tools available are sometimes considered obsolete or unsuitable (see IO.7). Although the DGJ has set up certain ad hoc programmes and bilateral cooperation initiatives, in particular with France, these efforts are still too limited to fully meet operational needs. With regard to TF, a financial investigation is conducted as part of each investigation to gain an understanding of the financing of terrorist activities, and the CTIF is systematically asked for any information it holds and for information from

its foreign counterparts. A full bank investigation is carried out as standard, including interviews with money transfer operator managers, in order to obtain an overview of the suspects' financial flows. If there are indications that the suspects have used cryptocurrencies, a search is also carried out on these exchange platforms. In addition, the judicial authority systematically requests technical assistance from the intelligence services in each new judicial case opened concerning terrorism and TF (see IO.9, circular COL 9/2012).

609. Furthermore, the financial intelligence obtained from cash movement reports available to the customs authorities is generally not used effectively by the investigative and prosecuting authorities. Despite this information being detailed (see section 6.3), it is still raw data that has not been refined through additional analysis, as customs authorities do not have investigative powers and are limited to recording incidents of non-compliance with reporting requirements. The number of ML investigations initiated as a result of customs offences is low (see IO.8). Given the prevalence of cash in ML/TF cases, the underutilisation of customs information by the judicial authorities is a significant shortcoming.

6.4.2. Use of financial information/intelligence to assist in identifying and tracing criminal proceeds or instrumentalities

610. Judicial and law enforcement authorities work closely together to identify and locate proceeds and instrumentalities of crime, building this into the early stages of investigations. However, the approach focuses on immediately available assets, which limits the broader identification of proceeds generated by ML activities. In-depth asset investigations are not conducted frequently enough, with the judicial authorities concentrating their investigations on the predicate offences without considering the ML aspects. This is due to insufficient resources (see IO.7 and IO.8).

7 Money laundering investigations and prosecutions

The relevant Immediate Outcome considered and assessed in this chapter is IO.7. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 3, 30, 31 and elements of R.1, 2, 15, 32, 37, 39 and 40.[166]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) Suspicious ML activities are mainly identified by police sources and, to a lesser extent, from STRs analyses submitted by the CTIF. The files that the CTIF forwards to the judicial authorities are not sufficiently used, due to insufficient capacity (see IO.6). The identification of ML cases is not based on a strategic approach and is only partially linked to the main risks to which Belgium is exposed.

b) Belgium does not give specific priority to prosecuting ML relating to the main predicate offences identified as being most at risk, i.e. drug trafficking, social and tax fraud.

c) The prioritisation criteria for initiating ML investigations (TRIM criteria), formalised in September 2022, do not adequately direct investigations and prosecutions towards handling complex ML cases and laundering of proceeds from predicate offences that generate significant financial flows. These criteria mainly address the need to optimise investigations in the context of persistent lack of human and technological resources allocated to the Belgian judicial system. A significant proportion of investigations focus on the underlying criminal facts, without in-depth financial investigation into money laundering.

d) The CTIF may request financial intelligence from its foreign counterparts following requests from the Belgian judicial authorities as part of ML proceedings. However, the CTIF only makes use of this option if it already holds information related to the request in its databases, which in some cases prevents the judicial authorities from speeding up the international cooperation process and supporting ML investigations with an international dimension.

[166] Recommendations 1, 2, 3, 15, 32 and 40 are under review, see Technical Compliance Annex.

e) The growing use of virtual assets in ML cases is a challenge that Belgian law enforcement authorities have identified and that requires innovative technical tools to which investigative authorities have limited access due to a lack of resources.

f) Belgium mainly prosecutes cases involving relatively simple typologies, such as 'money mules'. The number of cases closed without further action has increased in recent years, including for discretionary reasons linked to the lack of specialised investigators.

g) Some ML cases show that the authorities can prosecute complex forms of ML with an international dimension. These cases concern ML involving offsetting schemes in organised social fraud networks, identified by the CTIF and investigated mainly by the Federal Prosecutor's Office, and cases of drug trafficking and criminal organisations (e.g. the Sky ECC case). However, Belgium does not prioritise investigations into these complex cases, which account for only a limited proportion of convictions for ML.

h) The legal framework in Belgium allows for convictions for ML without having to establish a link between the predicate offence and the ML, which should make it easier to prove ML. However, this is not reflected in the number of convictions for ML (and the volume of confiscations, see IO.8). Although the number of convictions for ML has been increasing since 2019, these convictions are largely secured in domestic ML cases and are not fully aligned with the country's risk profile, particularly with regard to ML involving multiple offences and organised crime.

i) The sanctions imposed in ML cases are generally not effective or deterrent, which undermines the impact of the judicial system as a whole in dealing with ML cases. Insufficient resources mean that the Belgian authorities frequently resort to the transaction procedure, which, in addition to lacking a deterrent effect, is not an appropriate alternative criminal justice measure in ML cases.

Key Recommended Actions (KRAs)

Belgium should:

a) Allocate resources and effective technological tools to the authorities responsible for investigation and prosecution, commensurate with the threats identified, in order to tackle the polycriminal networks involved in ML.

b) Implement a proactive strategy for identifying ML and define a criminal justice policy that directs investigations and prosecutions towards complex ML cases with significant profits, in line with the ML risks identified, by relying on established jurisprudence on ML evidence (reversal of the burden of proof of the illegal origin of funds) and by enhancing the Federal Prosecutor's Office attributions to prosecute most complex ML cases to optimise handling of these cases.

c) Ensure that deterrent sanctions are imposed on criminals convicted of ML offences, and restrict the use of non trial resolution mechanism (the "transaction procedure") in ML cases, which must not replace criminal prosecution and must include guarantees of transparency and public disclosure of the agreements reached.

Other Recommended Actions

Belgium should:

a) Ensure that investigations and prosecutions of predicate offences systematically include an in-depth financial component for ML that identifies the broader pattern of criminal activity and illegal assets generated in ML cases.

b) Initiate ML investigations more systematically based on financial intelligence from the CTIF and information from other competent authorities.

c) Make strategic use of tax and customs information to initiate and enhance ML investigations, thereby enabling the prosecution of predicate offences related to tax fraud and cash trafficking, which are prevalent in Belgium.

d) Provide prosecutor's offices, in particular the Federal Prosecutor's Office, and investigating judges with financial analysts dedicated to ML investigations and prosecutions.

e) Increase operational training measures in financial crime investigations for investigators and financial analysts in both prosecutor's offices and the judicial police.

f) Encourage the CTIF to implement the ability to obtain financial intelligence from foreign FIUs to meet the needs of Belgian ML judicial proceedings, even when the CTIF does not already have information relevant to the subject of the request.

g) Ensure that the considerations taken into account by the prosecution services in charge of social frauds ("auditorats du travail") when deciding to initiate an ML investigation do not restrict the ability to prosecute cases where the illegal profits generated by social fraud are significant.

h) Strengthen financial analysis teams within the "auditorats du travail", where necessary, by making more systematic use of multidisciplinary investigation teams (MOTEM).

i) Ensure that the process for formally bringing charges in ML cases does not unreasonably impact the length of proceedings.

Overall Conclusions on IO.7

The Belgian authorities have demonstrated, to some extent, their ability to prosecute and obtain convictions in complex ML cases. However, Belgium does not give priority to these types of ML investigations, despite the country's identified exposure to ML schemes involving polycriminal ML schemes and organised crime.

The lack of human resources, specialisation and access to sophisticated technological tools significantly hinders Belgium's efforts to effectively combat the large-scale criminal activities the country faces. The authorities do not have a strategic approach, the financial resources or adequate technical capabilities to identify, investigate and prosecute ML cases in a way that is commensurate with the high risks to which Belgium is exposed. The lack of resources affects how ML cases are handled throughout the criminal justice system and forces the Belgian authorities not to open certain investigations, to close them without further action for discretionary reasons linked to resources, and to resort to transaction agreements to resolve these cases. In 2015, the FATF noted the consequences of the significant lack of resources affecting the country's ability to effectively tackle ML and predicate criminal offences. However, these shortcomings persist.

Major improvements are required.

Belgium is rated as having a Moderate level of effectiveness for IO.7.

Immediate Outcome 7

611. The evaluation team has based its conclusions on case examples provided by the authorities, statistical data available to Belgium, and numerous interviews with Belgian authorities during the on-site visit (see the Introduction for a description of the institutional framework).

612. The lack of granularity and completeness of statistics on ML investigations, prosecutions and sanctions makes it impossible to break down the data by predicate offences or to distinguish between convictions by ML type.[167]

7.1. ML activity identified and investigated

7.1.1. Identification of ML cases

613. Suspicious ML activities are mainly identified by police sources based on incidental findings in the course of criminal investigations (accounting for 57% of cases referred to prosecutor's offices).[168] A significant proportion of these cases are small-scale and typically involve, for example, 'money mules'.[169] ML investigations were initiated following the decryption of a large number of communications from the Sky ECC platform (see box below), made possible by Europol and Eurojust's financial and technological support. The information provided by the CTIF has led to a lower proportion of investigations being opened by prosecutor's offices (approximately 17% of cases referred to prosecutor's offices). The number of files forwarded by the CTIF to the judicial authorities based on the analyses of suspicious transaction reports (STRs) has remained stable since 2020. A total of 6,389 new files were forwarded between 2020 and 2024 (see IO.6)[170] Most of these files involve potential predicate criminal offences linked to fraud, organised crime, serious tax fraud, social security fraud and drug trafficking.[171] However, this source is not used to its full potential by the investigative and prosecuting authorities. A significant proportion of these referrals do not lead to the opening of an investigation, mainly due to a lack of resources and ability to seize illicit funds when they are not directly available, e.g. if they are located abroad, in accordance with the TRIM criteria (see section below). Between 2019 and 2024, 43% of files forwarded by the CTIF to the judicial authorities were closed without further action, raising concerns that a significant proportion of CTIF communications are not being fully utilised.

614. *Strengthening the detection of ML activity* was identified as a priority area in the AML Action Plan adopted in March 2024 (see IO.1). However, this priority has not resulted in practical measures such as developing a strategic framework and allocating human and technological resources to support a stronger and more targeted approach to identifying ML cases. In practice, Belgium does not apply a strategic approach to identifying ML activity that is commensurate with the risks to which the country is exposed, in particular those related to the existence of organised networks, professional ML involving multiple criminal offences, the widespread use of cash, the diamond sector and illegal activities generating funds that are laundered outside the financial system (see IO.1). The FATF noted weaknesses in identifying money laundering cases back in 2015. The Belgian authorities have since become aware of the growing scale of criminal activities that could undermine the fundamental foundations of Belgian society and their potential

[167] There are legal and regulatory requirements for keeping these statistics in Belgium, but they have not been implemented (see TC Annex, R 33).

[168] Database of the College of Prosecutors General – statistical analysts

[169] Annual Report 2024 of the Public Prosecutor's Office. The use of money mules was also highlighted in the typologies identified in the SKY ECC case. In addition, the findings of the Annual Report 2024 show an increase in files relating to the offences of concealing stolen goods and money laundering, which the authorities attribute mainly to the phenomenon of money mules or financial mules.

[170] CTIF Annual Report 2023, p. 35 and CTIF Annual Report 2021, p. 39.

[171] CTIF Annual Report 2023, pp. 50-52.

repercussions at the international level, particularly in neighbouring countries. However, Belgium has not stepped up its response to the high risks to which the country is exposed in order to identify ML activities in a more targeted and proactive way.

615. *The allocation of ML cases* to the various district prosecutor's offices is based on territorial distribution criteria that have an impact on the subsequent judicial handling of cases. This allocation does not always make it possible to identify and deal in a coordinated manner with related cases opened in several prosecutor's offices, due to a lack of coordination between these offices. The operational limitations of the database that lists cases opened in the various prosecutor's offices and police departments hinder operational coordination, as noted by the federal authorities.[172] Identifying links between different cases is random and should be improved to make it easier for Belgium to tackle offences involving multiple crimes across the country. New tools have been introduced to streamline the digital processing of files, but their recent rollout means that it is too early to measure their impact.[173]

Box 7.1. The SKY ECC case

The SKY ECC case demonstrates Belgium's ability to identify ML cases involving significant financial flows with international connections. It illustrates the authorities' ability to reorganise their operational framework to maximise the expertise available at federal and local level and the importance of the CTIF as a source of financial intelligence.

The case originated with the interception, decryption and utilisation of data from the SKY ECC encrypted communication system used by numerous criminal networks. Analyses of the decrypted data revealed the extent of the criminal networks involved in drug trafficking in Belgium, the prevalence of the use of cash and money mules, and the growing use of virtual assets, particularly for transferring illegal assets out of Belgium. Financial flows mainly transit through Belgium to the countries of origin of those involved, but are also invested directly and laundered within Belgium.

This case, which the Federal Judicial Police started in early 2021, led to the opening of a total of 643 judicial investigations under the name 'Operation Edge', including 442 new and 201 existing investigations that were expanded after the data was decrypted. Two thirds of the investigations (439 cases) involve drug trafficking and 63 involve ML offences.

In response to the scale of the criminal activities identified, Belgium has reorganised its operational framework to split up and coordinate the various investigations between the federal police and local police forces and to allocate cases between the Federal Prosecutor's Office and district prosecutor's offices. The Federal Prosecutor's Office has focused its efforts on recovering assets abroad and extraditing suspects. A stronger communication framework has also been put in place with the CTIF (see IO.6).

Prosecution proceedings have been initiated and 131 judgements have been handed down to date, with more than 1,093 people convicted, all offences combined. The case has also resulted in convictions for ML, although the exact number of these was not shared with the evaluation team. .

Based on an analyses of 75 court cases from Sky ECC, the Federal Judicial Police (DJSOC) conducted an internal analyses in 2024 to identify trends and modus operandi in these cases.

616. *The allocation of cases between the Federal Prosecutor's Office and district prosecutor's offices* does not follow clearly established criteria. The Federal Prosecutor's Office has concurrent and subsidiary

[172] Evaluation Report of Belgium (2015), p. 61.

[173] JustOne and JustCase.

jurisdiction over district prosecutors in ML matters. A College of Prosecutors General circular[174] and the 2021 Priority Note from the Public Prosecutor's Office stipulate that the Federal Prosecutor's Office has jurisdiction over ML cases involving offsetting schemes and plays a coordinating role in cases handled by district prosecutors relating to criminal organisations with international connections. The Federal Prosecutor's Office may also take on complex ML cases where it wishes to develop innovative investigation methods or tackle certain criminal phenomena. District prosecutor's offices have indicated that they do not always understand the scope and characteristics of the cases taken on by the Federal Prosecutor's Office. One case illustrates how the transfer to the Federal Prosecutor's Office of several cases handled by district prosecutor's offices led to the identification and dismantling of a complex ML case involving an offsetting scheme (the Clown case, see box below). However, Belgium has not adopted a systematic approach to joining related money laundering cases with a view to dismantling criminal networks. The powers and functions of the Federal Prosecutor's Office to deal with complex ML cases with an international dimension and involving significant financial flows have therefore not been fully optimised. The least well-resourced prosecutor's offices do not seem to be able to call on those with more resources and expertise to deal with more complex cases.

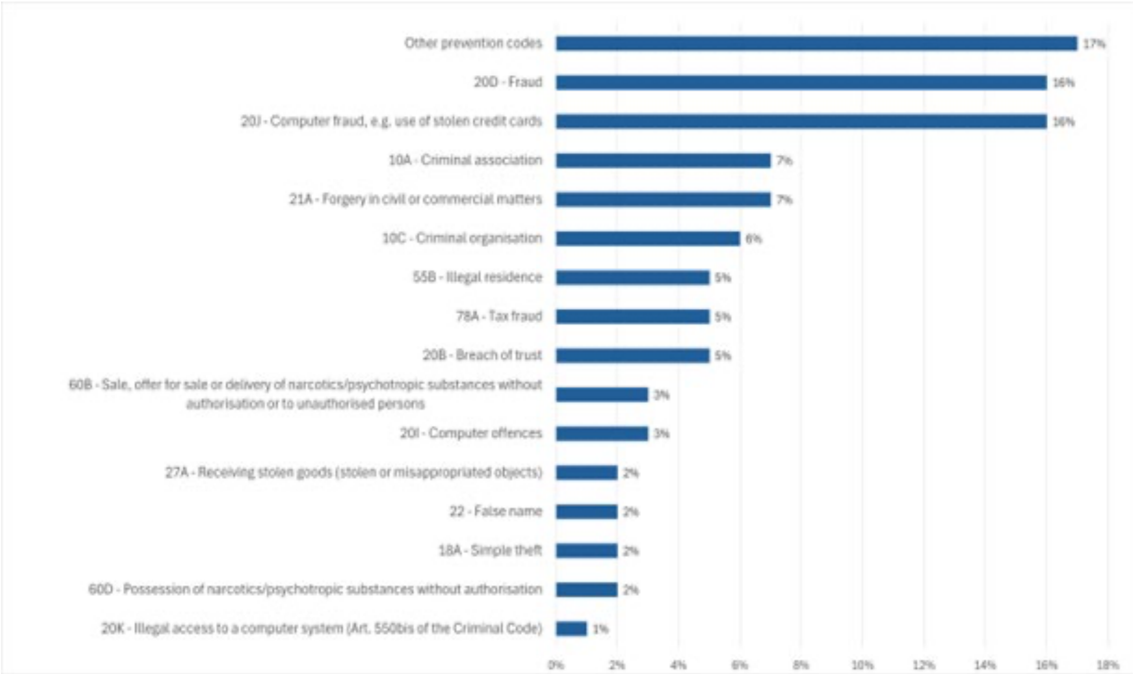
7.1.2. ML investigations

617. Approximately 400 new cases were opened each year by the Federal Judicial Police (FJP) between 2019 and 2024. Almost a quarter of these criminal investigations opened in 2023 involved drug trafficking, largely based on information from the Sky ECC case (see box above). However, these investigations do not necessarily include money laundering aspects.

618. In January 2025, out of a total of 10 868 cases referred to prosecutor's offices, 5 782 ML cases were police investigation awaiting a decision on how to proceed, and 984 cases (representing 2.3% of cases referred to prosecutor's offices) were the subject of a judicial investigation (including cases awaiting formal charges prior to referral to a court).

[174] COL 14/2022

Figure 7.1. Most frequent predicate offences recorded by prosecutor's offices in ML cases opened between 1 January 2019 and 31 December 2024



Note: The unit of measurement in this graph is not the number of criminal cases but the number of 27b prevention codes (corresponding to ML). These figures should be treated with caution, as the predicate offences are not always identified when a case is opened and therefore not always recorded, and records are not necessarily updated during the investigation.
Source: Database of the College of Prosecutors General – statistical analysts

619. Some cases presented to the evaluation team show that the Belgian authorities have the ability to investigate complex forms of ML, some of which have an international dimension. However, Belgium does not give specific priority to these types of ML investigations, despite the high risks to which the country is exposed. Investigations mainly focus on ML offences committed in Belgium in connection with predicate offences also committed in Belgium, as previously noted in the FATF's 2015 evaluation report.

620. Belgium also does not appear to prioritise investigations into predicate offences that generate significant profits and pose a significant risk in Belgium, such as drug trafficking and tax and social security fraud (see chart above). However, these were identified as priority criminal activities by the Public Prosecutor's Office in 2021, in line with the findings of the ML NRA (see the Introduction).[175] Money laundering is also identified, but it is not correlated with the various forms of predicate offences. Only ML derived from frauds other than tax and social frauds also identified as a prevalent predicate offence in Belgium, ranks second in the ML investigations initiated during the period under review.

621. In practice, a significant proportion of investigations focus on *establishing the facts of the predicate offences*, without conducting an in-depth financial investigation into ML, which also impacts Belgium's ability to deprive criminals of the illegal assets obtained (see IO.8). The investigative and prosecuting authorities are aware of the importance of conducting financial investigations into ML, but cite a lack of human and technological resources as the reason for this approach. As a result, some prosecutor's offices consider that it is neither appropriate nor effective to prosecute the ML offence and prefer to seize the

[175] Priority note from the Public Prosecutor's Office (2021)

value of the illegal gains generated by the predicate offence. The Federal Judicial Police's Internal Directive of January 2022, on economic and financial crime and the approach focused on the confiscation of criminal proceeds ('spoils-focused'), emphasises the importance of stepping up the opening of ML investigations. In particular, it recommends setting up teams specialising in the search for illegally acquired assets (PLUK teams) to support investigations in priority areas such as drug trafficking (see IO.8). However, implementing these guidelines requires adequate human and technological resources, which they currently do not have.

622. *Drug trafficking* is one of the most prevalent forms of crime in Belgium (see IO.1). However, the volume and characteristics of investigations opened into ML linked to this trafficking are not commensurate with the significant risk to which Belgium is exposed, despite the Public Prosecutor's observation that large amounts of money are being laundered in this way. These investigations do not therefore achieve the objective set by the Public Prosecutor's Office of financially dismantling criminal networks, even though this trafficking is often part of wider professional ML and offsetting mechanisms. It is symptomatic that the remit of the National Drug Commission, created in January 2023, was only extended in early 2025 to include ML, reflecting the lack of priority given to tackling the money laundering of proceeds from drug trafficking until then.

623. The Public Prosecutor's Office identified *organised crime* as a priority criminal activity in 2021 and set itself the objective of dismantling criminal structures by applying 'a long-term investigation strategy [that] must not only lead to the prosecution of individuals who have committed specific offences, but also bring the real organisers of criminal networks to justice'.[176] However, these objectives are not reflected in investigations and prosecutions, which often focus on perpetrators at the bottom of the chain. The criteria guiding the opening of ML investigations also do not provide incentives to undertake long-term investigations (see below).

624. The more complex files handled by Belgium include *ML cases involving offsetting schemes*, initially identified by the CTIF and investigated mainly by the Federal Prosecutor's Office, particularly with a view to dismantling networks involved in organised social security fraud (see IO.1). A notable example is the 'Clown' case.

[176] Priority note from the Public Prosecutor's Office

Box 7.2. Clown' case[177]

This case demonstrates the ability of the Federal Prosecutor's Office to investigate complex ML cases involving offsetting schemes with an international dimension. The case was initially investigated over several years by various prosecutor's offices and "auditorats du travail",[178] without any connection initially being made between the various cases. However, the criminal activities were part of a more complex ML scheme that was identified when the Federal Prosecutor's Office brought the investigation under federal jurisdiction following an exchange with one of the investigating judges. The ML scheme had been developed as part of a criminal organisation enabling illegal funds from cash-generating criminal circles (such as drugs and prostitution) to be made available to criminals whose illegal activities generate a need for cash (in this instance for social security fraud in the construction and cleaning sectors). Several CTIF reports sent to prosecutor's offices and the "auditorats du travail" in several districts between 2015 and 2019 shed light on this scheme.

The Federal Prosecutor's Office took over the investigation of the case in 2018 as part of a multidisciplinary investigation involving, among others, the social security inspectorates. Bringing the case under federal jurisdiction meant that the CTIF reports could be consolidated to trace the suspicious financial flows, estimated at over EUR 80 million. It also allowed the Prosecutor's Office to expand the investigation into ML and organised crime, using evidence gathered during social security fraud investigations previously conducted by district prosecutors and the "auditorats du travail".

Convictions for autonomous ML were upheld on appeal in March 2023 against three of the defendants, with a seven-year prison sentence for the main defendant and suspended sentences for the other two defendants (four and five years respectively, suspended for five years). Equivalent-value confiscation orders were also handed down (between EUR 1 million and EUR 350 000), but the amounts were reduced by the judge to take into account the need to impose reasonable sentences (Art. 505(6) and (7) of the Penal Code).

7.1.3. Discretionary investigation of ML cases

625. Belgian criminal procedure is governed by the principle of discretionary prosecution. Investigation priorities for ML cases are set by the *Target, Recoup, Impact, Mode* (TRIM) criteria adopted by the College of Prosecutors General in 2022.[179] These criteria were developed based on the approach followed by the prosecutor's offices and in response to the FATF's recommendations in the 2015 MER.[180] They also serve to determine whether proceedings should be discontinued, even if there are grounds for suspecting that a money laundering offence has been committed.

626. These TRIM criteria primarily reflect a need to optimise the judicial handling of ML cases in the context of the persistent lack of resource allocated to the Belgian judicial system. They are not sufficient to effectively focus investigations and prosecutions on complex ML cases and predicate offences involving large amounts of money, commensurate with the prevailing ML risks to which Belgium is exposed.

627. While the significance and weight of ML risks may be reflected in the criteria (primarily the *Impact* one relating to the seriousness of the predicate offence), in practice, the main criterion for determining

[177] Mons Court of Appeal ruling of 17 March 2023, FD.10.98.481/18.

[178] When laundering is linked to social security fraud, it is the labour prosecution service (the "auditorats", who are specialised public prosecutors) that handle money laundering cases.

[179] COL 14/2022

[180] FATF Mutual Evaluation Report of Belgium, 2015, p. 58.

whether to open an investigation and prosecute is *R(ecoup)*, which relates to the likelihood of recovering property or financial gains (in addition to the available police resources, see below).

628. The central test is the ability to *recover assets or financial gains of criminal origin (Recoup)*, which determines whether it is worthwhile opening an investigation. However, the restrictive way in which this criterion is applied means that prosecutors and investigators are steered towards cases where ML assets and proceeds are easily and immediately accessible at the start of the investigation, which prevents the consideration of the financial volumes generated by the offences in their entirety. This approach means that the handling of ML cases involving complex financial schemes, where in-depth investigations are necessary to determine the extent of the profits generated by criminal activity, is not always prioritised. When assets and/or proceeds obtained through ML are located abroad, recovery is more difficult, and prosecutors often prefer to refer the cases to foreign authorities, which are better placed to prosecute the perpetrators, particularly in view of the difficulties encountered in international cooperation with certain foreign authorities (see IO.2).

629. The *issue of police resources (primarily specialised investigators)* is also a determining factor in the decision to open or close a ML investigation. Without adequate police resources to conduct investigations within a reasonable time frame, cases are likely to be closed on discretionary grounds without criminal prosecution.

630. Although considerations relating to the importance of prosecuting the person (*Target*), the damage caused by the ML offence (*Impact*) and the organised nature of the ML offence (*Mode*) are included in the TRIM criteria, they appear to be given secondary consideration compared to the *Recoup* criterion. In any event, it appears that the TRIM criteria filter is applied at an early stage, which does not provide a sufficiently in-depth view of the factual elements of the suspected ML activities that should guide the decision to open an investigation.

631. The TRIM circular also recommends avoiding ML cases involving a wide range of offences, the handling of which would extend the investigation period beyond a reasonable time frame (so-called 'mammoth' cases). In practice, cases are split up and focus on the aspects of the case where the facts are most clearly defined and the suspects identified. While this approach appears pragmatic given the limited resources available, it is not an optimal way to tackle cases involving active polycriminal networks in Belgium.

632. In ML cases involving social security fraud, the "*auditorats du travail*" (public prosecutors specialising in social security fraud and ML) apply similar criteria when deciding how to proceed with ML cases, which are usually instigated based on a report submitted by the CTIF. Cases are handled depending on whether there are signs of social security fraud, whether the suspects are already under investigation by the "*auditorat*" and depending on the available investigative resources of the social security inspection and police services or the designated judge. In practice, the Brussels "*auditorat*" also takes into account the estimated amount of social security fraud and only opens an ML investigation if this amount exceeds EUR 500 000, due to a lack of adequate resources. This threshold seems too high and is likely to limit the effectiveness of Belgium's enforcement efforts against social security fraud, which has been identified as a significant risk area in Belgium.

7.1.4. ML investigation techniques and framework

633. The authorities have access to a large number of *databases and financial information* held by the CTIF (see IO.6). The judicial authorities ask the CTIF to provide them with any relevant information it holds and send it requests for information and financial analyses.[181] Where the request from the judicial

[181] Art. 84 para. 1 of the AML Law

authorities involves contacting foreign FIUs, the CTIF has the power to approach its foreign counterparts.[182] In practice, however, the CTIF only uses of this faculty for ML cases if it already has related information based on STR received and its own analyses. This approach limits informal cooperation and access to financial intelligence located abroad, thereby preventing judicial authorities from speeding up the international cooperation process and supporting ML investigations with international connections to which Belgium should give priority (see IO.2). Furthermore, the *financial information held by the tax authorities* (see IO.6) and *customs authorities* (see IO.8) is not sufficiently analysed and exploited to prosecute ML. One isolated high-profile case illustrates how the information held by the customs authorities can lead to ML convictions (see the box on the Pondjes case in section 7.3).

634. The *judicial investigative authorities* use various investigative techniques, in particular the special investigative techniques at their disposal, including intercepting phone calls. The dismantling of the Sky ECC encrypted messaging platform used by many criminal networks has provided access to many sources of information used in investigations since 2021. However, the increasing use, identified by law enforcement agencies, of virtual assets in ML cases is a challenge that requires innovative tools to which investigative authorities have a limited access due to a lack of resources. In more complex cases, the Belgian authorities frequently resort to international cooperation, particularly when assets derived from ML are located abroad. They also participate in joint investigation teams with other European authorities. However, mutual assistance with certain non-EU third countries to which assets derived from ML are mainly redirected is complex, and prosecutors have reported that it is difficult to obtain cooperation from authorities in these countries. Recently, steps have been taken to overcome these obstacles (see IO.2).

635. For *social security and tax fraud investigations*,[183] the prosecutor's office has been able to call on multidisciplinary investigation teams (MOTEM) since 2019 and 2022 respectively. These investigation teams are set up on an *ad hoc* basis for a relatively short period of time (e.g. six months). They allow prosecutor's offices to tap into specialist expertise and make up for shortcomings in police resources by seconding tax experts and investigators from social security inspection departments. In practice, the use of MOTEM is limited and has not yet delivered tangible results in ML investigations. Only 33 MOTEM were set up in tax investigations started between 2023 and 2024, including 10 cases where ML was specifically targeted. Three of these MOTEM came to an end in 2024, without any ML evidence being substantiated. The majority of these investigations are still ongoing and it is therefore too early to draw conclusions on the impact of MOTEM in ML cases.

7.1.5. ML cases referred to investigating judges

636. Since 2019, the proportion of ML cases in which an investigating judge has been assigned is relatively low compared with other types of cases and the number of cases closed without further action. However, a number of investigative measures cannot be ordered outside the framework of a judicial investigation. In general, ML cases do not appear to be subject to in-depth investigation at the police investigation stage, prior to the opening of a judicial investigation.

637. This finding is consistent with the lack of specialised resources available due to insufficient police capacity to carry out the investigative measures ordered. Fewer than 10% of the 42 115 ML cases filed with prosecutor's offices between 2019 and 2024 were referred for judicial investigation. Cases handled by the "*auditorats du travail*" (related to social security offences) follow the same trend, with fewer than 5% of the 1 541 cases filed with labour prosecution offices progressing to the formal ML investigation stage between

---

[182] Art. 123 of the AML Law

[183] In tax fraud cases, the following factors will be considered when deciding whether to set up a MOTEM: the seriousness of the offences; the existence of serious indications that the offences are used to finance a criminal organisation; an international dimension; and the use of judicial investigation measures involving coercive measures. The prospect of seizing sums of money and crypto-assets is not a criterion for forming a MOTEM but is a determining factor in assessing the 'profitability' of the investigation.

2020 and 2024. However, the most complex ML cases, which generate significant profits, require investigative measures that can only be ordered by an investigating judge (e.g. searches, detention, etc.).

638. The Belgian authorities have investigated ML cases with international connections, with a total of 345 cases under formal investigation between 2019 and 2023, mainly conducted by the prosecutor's offices in Brussels and Antwerp. However, Belgium does not provide information on the type of cases, the predicate offences targeted, or whether these investigations led to formal prosecutions and eventual convictions.

7.1.6. Resources and specialisation

639. The investigative and prosecuting authorities do not have adequate financial and technical resources to identify and investigate ML cases generating significant profits. In 2015, the FATF noted the significant lack of resources affecting the country's ability to effectively tackle ML and predicate criminal offences. A 2023 European Commission report also highlights persistent resource gaps affecting the Belgian judicial system.[184] In light of this, the efforts of law enforcement agencies to take action against ML offences are commendable but remain insufficient, as they have been working at maximum capacity for years.

640. The Federal Judicial Police does not have sufficient human resources to carry out the investigations required by all district prosecutor's offices, the Federal Prosecutor's Office and the delegated prosecutors of the European Public Prosecutor's Office (EPPO). Approximately 560 investigators specialising in financial matters are employed in the 14 Federal Judicial Police investigation units. The Judicial Police Directorate-General (DGJ) has reported persistent difficulties in recruiting specialised staff with economic and financial skills due to the unattractive nature of the profession. The police training programme has been strengthened since 2022 with the introduction of an annual round of specialised training courses on ECOFIN, which was extended to members of the judiciary in 2024. This training, delivered by external third parties rather than peers, focuses mainly on the legal framework and certain ML practices. However, it is not adequately geared towards developing the operational and strategic capabilities of the authorities responsible for ML investigations and prosecutions.

641. At the prosecutor's office level, specialised ECOFIN sections deal with ML and economic and financial crime cases. However, unlike the EPPO's delegated prosecutors, these prosecutor's offices do not have their own financial analysts. The ECOFIN section of the Antwerp prosecutor's office has only seven prosecutors, three of whom are specialised in tax matters. The Brussels prosecutor's office has only nine prosecutors, and the Liège and Mons prosecutor's offices have three prosecutors each. The sheer number of open files handled by each prosecutor makes it impossible to deal with complex ML cases. Only three investigating judges out of a total of 17 in Belgium specialise in financial matters, which is too few.[185]

642. The lack of staff, specialisation and access to effective technological tools, particularly for police authorities, places a significant constraint on ML investigations and has repercussions throughout the judicial process.

643. The significant proportion of ML cases that are closed without further action is also linked to the lack of resources allocated to the judicial authorities and impacts Belgium's ability to deal successfully with important ML cases. Between 2019 and 2024, 19 212 cases were closed without further action by all prosecutor's offices combined, equivalent to almost 46% of ML cases recorded by prosecutor's offices. This finding is all the more worrying given that 7 896 of these cases (nearly 19% of those recorded by prosecutor's offices) were closed for reasons of expediency, mainly due to insufficient investigative

[184] European Commission, 2023 Rule of Law Report – Belgium, pp. 3, 7-8; An OECD report published in March 2025 also highlights these shortcomings.

[185] Mutual Evaluation Report of Belgium (2025), para. 119). OCDE (2025), *OECD Anti-Bribery Convention – Phase 4 Report on Belgium:Implementing the Convention and Related Legal Instruments*, Implementation of the OECD Anti-Bribery Convention, OECD Publishing, Paris

capacity. The same observation applies to cases brought before the "*auditorats du travail*": between 2019 and 2024, 1 035 of the 1 984 ML cases recorded were closed without further action (52% of cases). Of these 1 035 cases closed without further action, 643 were closed for discretionary reasons (more than half of the cases closed without further action).

644. A limited number of cases (around 2% of cases brought before prosecutor's offices between 2019 and 2024) are classified under the 'judicial probation' ("*probation prétorienne*") mechanism (formal caution with conditional dismissal). The suspect is told that they have committed an offence. No criminal proceedings are brought, provided that the suspect does not reoffend and complies with any conditions set by the prosecutor's office.

645. The lack of resources has an impact beyond the law enforcement agencies and undermines the impact of the CTIF's actions, as the authorities responsible for investigations do not have the capacity to fully follow up on the information provided by the CTIF (see section 7.1). The 2015 FATF report highlighted the concerns raised by the CTIF since 1996 about the judicial treatment of ML cases referred by the CTIF.[186] The impact of the lack of resources also affects Belgium's ability to conduct in-depth financial investigations to seize and confiscate criminal assets obtained through ML (see IO.8).

7.2. Prosecuting and convicting different types of ML activities[187]

7.2.1. Prosecutions

646. Between 2019 and 2024, the Belgian authorities prosecuted 2 455 ML cases (less than 6% of the total number of cases referred to prosecutor's offices). In line with the findings relating to investigations, Belgium prosecutes a small proportion of money laundering cases, whose profile is not entirely consistent with the main types of criminality (i.e. drug trafficking, social security and tax fraud). The proportion of cases prosecuted for autonomous ML is not known. ML cases resulting in prosecution are relatively less complex and mainly concern domestic ML. Based on the cases presented, the majority of ML prosecutions and convictions relate to self-laundering and to perpetrators at the bottom of the criminal chain. Belgium does not prioritise the tackling of criminal networks, although some complex cases involving criminal organisations have been taken to court and resulted in convictions.

647. Major cases exposing offsetting schemes and drug trafficking (Sky ECC) have resulted in prosecutions and convictions, demonstrating that the authorities are capable of prosecuting complex ML cases generating significant profits (see boxes on the Clown and Pondjes cases). However, Belgium lacks the strategy and resources to prioritise these cases.

648. The legal framework in Belgium allows ML cases to be prosecuted and convictions handed down without having to prove the predicate offence. According to established case law,[188] it is only necessary to demonstrate beyond reasonable doubt that the financial gains have no lawful origin, which reverses the burden of proof to some extent. This framework should make it easier to prove ML, particularly ML as a stand-alone offence, and optimise the use of resources allocated to prosecuting ML. The opportunity to treat ML as a standalone offence is addressed in the TRIM circular. However, the authorities do not make sufficient use of this , even though it would make it easier to prosecute ML, particularly for predicate offences committed abroad.

---

[186] Mutual Evaluation Report of Belgium (2015), p. 64, para. 3.71). OCDE (2025), *OECD Anti-Bribery Convention – Phase 4 Report on Belgium:Implementing the Convention and Related Legal Instruments*, Implementation of the OECD Anti-Bribery Convention, OECD Publishing, Paris

[187] See Methodology, IO.7, Note for evaluators 2 and associated footnotes.

[188] Belgian Court of Cassation, 17 December 2013, P.13.1354.N.

Box 7.3. Court of Cassation case law on the exclusion of lawful origin

The Belgian Court of Cassation has consistently held that sums of money converted and/or invested which cannot be proven, based on the circumstances of the case (factual assessment), to have been obtained through legal activities, constitute financial gains of unlawful origin, the concealment or disguise of which constitutes money laundering (see, in particular, Cass., 21 March 2006, RG. no. P.06.0034.N, Pas., 2006, 165; Cass., 12 June 2013, RG no. P.13.0312.F, Pas. 2013, 363; Cass., 5 February 2019, RG no. P.18.1010.N).

For example, the Court of Cassation ruled that 'in order for the perpetrator of ML offences within the meaning of Article 505, paragraph 1, points 2°, 3° and 4° of the Penal Code to be found guilty and convicted, it is sufficient that the unlawful provenance or origin of the items referred to in Article 42, point 3°, of the Penal Code and the perpetrator's knowledge thereof be established, without it being necessary for the criminal court to know the specific offence, provided that, based on the facts, the court can rule out any lawful provenance or origin. (...) The unlawful origin of the items may also be inferred from the fact that there is no credible evidence that their origin may be lawful.' (Cass., 17 December 2013, RG no. P.13.1354.N).

649. Lastly, procedural aspects at the stage when formal charges are brought (before the "Chambre du conseil" and the "Chambre des Mises en Accusation") slow down the progress of prosecutions. On average, it takes two years before a case is referred to a court at that stage of the proceedings. The lack of procedural time limits before these Chambers allows the defence to lodge multiple appeals, resulting in sometimes significant delays in the processing of cases. Added to this are the times for bringing cases before the courts, which can take another year in the district of Liège, for example.

7.2.2. Convictions

650. The number of natural persons convicted of ML has increased since 2019 (see table below). However, this increase in numbers should be considered with caution as these convictions are largely obtained in relatively straightforward domestic ML cases. The information provided does not reveal whether Belgium prosecutes and hands down convictions for different types of money laundering, including autonomous ML, self-laundering, ML by a third party, and ML of proceeds from predicate offences committed abroad. Belgium has also not provided figures on the number of cases dismissed or resulting in acquittals.

651. A small number of legal persons have been convicted since 2021. Proportionally, convictions of legal persons account for around 3% of total convictions handed down between 2022 and 2024. This proportion reflects the fact that legal entities are most often mere vehicles with no real economic substance, created deliberately by natural persons and which may have ceased to exist and no longer have any funds at the time of criminal proceedings.

Table 7.1. Number of persons convicted for ML

	2019	2020	2021	2022	2023	2024* (estimate)	Total
Persons convicted		287	803	1 005	879	769	**3 743**
Of which natural persons		-	758	983	860	725	**3 326**
Of which legal persons		-	45	22	19	44	**130**

Note: Offences committed for attempted ML are included in these figures.
*Data for 2024 is not yet complete
Source: Criminal Policy Department – Criminal Records.

Box 7.4. Pondjes Case

This case illustrates Belgium's ability to detect ML activities involving offsetting schemes, estimated to be worth at least EUR26.5 million and linked to an international criminal organisation following the perpetration of customs offences, and to secure convictions, although some of the sanctions imposed are relatively lenient. An investigation was opened in November 2019 by the Brussels Halle Vilvoorde prosecutor's office into the activities of criminal organisations and ML, following the interception by customs officials of six cash couriers at Zaventem airport who were flying to Turkey.

In June 2024, the Brussels Court of First Instance convicted 78 of the 81 defendants. The three leaders of the criminal organisation were sentenced to seven to ten years' imprisonment, while the other defendants received sentences of one to four years, some with partial suspension. Fines were imposed ranging from EUR 16,000 to EUR200,000. Confiscation orders were made for £935,695 in undeclared cash, as well as equivalent-value confiscations of over EUR 26.5 million.

7.3. Effectiveness, proportionality and dissuasiveness of sanctions

652. The lack of data on the sanctions imposed does not allow to provide a comprehensive view of the level of punishment and their deterrent effect, by type of ML (i.e. self-laundering, autonomous ML, ML by a third party and complex ML). However, the judgements provided by Belgium reveal certain trends in the nature and level of sanctions imposed in ML cases.

653. Based on these judgements, it appears that the majority of sanctions imposed are neither effective nor dissuasive. Prison sentences are generally in the range of a few months to two years. They are frequently suspended in whole or in part, or sentencing is deferred entirely,[189] and these are usually accompanied by fines that have little deterrent effect (below EUR10,000) and are also suspended. These sanctions are not commensurate with the significant aggravating circumstances generally noted by judges in these cases, such as the seriousness of the offences, the amounts involved, including in cases where a significant profit was made from the offence, the length of the period during which the offence was committed, the degree of harm caused to Belgian society, and the defendants' lack of awareness of the seriousness of their actions. Exceeding the reasonable time limit also frequently affects the level of sanctions imposed.

[189] Deferred sentencing means that the judge considers the charges against the defendants proven but defers pronouncing the sentence for a period of one to five years depending on the facts (probationary period). If the defendants commit new offences during this period that result in conviction, the initial deferral may be revoked (i.e. the judge will then also impose a sentence for the original offence).

Box 7.5. Case B and G

Case B

In this case, the defendants were given suspended sentences with probation and independent community service orders instead of prison sentences, even though they were repeat offenders and the total amount laundered was estimated at over EUR 33 million.

Case G. Impact of exceeding the reasonable time limit

In this case, the defendant G., a natural person, was given an 18-month suspended prison sentence on the grounds that the reasonable time limit had been exceeded, as well as being barred from practising his profession, also suspended. However, the value of the illegal assets in this case amounted to more than EUR20 million in jewellery.

654. Cases in which prison sentences and higher fines have been handed down were mainly based on multiple offences committed by the defendants, for example human trafficking for economic gain.

655. Heavy sanctions have also been handed down in certain complex cases, including prison sentences (sometimes ranging from 7 to 10 years) and higher fines (see box on the Clown case and another case heard by the Namur Court of First Instance (November 2021) in which a fine of EUR600 000, together with a five-year suspension of half the fine, was handed down for ML of organised social security fraud). These heavier sanctions can be explained in part by the fact that the offences were deemed to constitute organised crime and by the number of offences for which the defendants were found guilty.

656. The sanctions imposed on the 130 legal persons convicted between 2019 and 2024 are unknown. The Belgian authorities provided two judgements in which legal persons were convicted of ML. The fines in these two cases are at the lower end of the applicable range (see Rec. 3 in the TC Annex). The fines range from EUR 72 000 to EUR 120 000, while the legal maximum is EUR 960 000, which has little deterrent effect in itself. These fines are also accompanied by a three-year suspension of half of the fine. However, the limited information provided does not allow for a more comprehensive assessment of the effectiveness and dissuasive effect of the sanctions imposed on legal persons found guilty of ML.

657. The *enforcement of criminal fines* in general is also problematic in Belgium, according to a report published in July 2023 by the Court of Auditors,[190] which also reduces the deterrent effect of the fines imposed. The report highlights the lack of tools to monitor the process of enforcing criminal fines and the risk of incomplete enforcement of judgements resulting from insufficient automation. The collection rates for fines imposed are low. The same challenges apply to the actual recovery of confiscated assets, the amounts of which are also frequently reduced by the courts. (see IO.8). Given these circumstances, the very prospect of being convicted does not act as a deterrent.

[190] Court of Auditors Report (July 2023) Enforcement of criminal fines – Follow-up in 2021 and 2023 of the recommendations of the 2019 audit.

7.4. Use of alternative measures

658. Belgium has not demonstrated its use of other criminal justice measures in cases where an ML investigation has been conducted but where a conviction for ML is not possible.

7.4.1. Use of non-trial resolution mechanism (the transaction procedure)

659. Belgium frequently uses the non-trial resolution mechanism – transaction procedure - for ML offences, as provided for in its Code of Criminal Procedure (Art. 216bis) and whose framework and conditions are set out in a circular issued by the College of Prosecutors General in 2018.[191] [192] Between 2019 and 2024, 390 transactions were agreed in ML cases at the preliminary investigative stage (simple transactions, not included in the person's criminal record). In practice, the majority of transactions are struck after criminal proceedings have been initiated (known as extended transactions), either when the proceedings are settled at the end of the investigation or when the case is brought before the court of first instance. Belgium was unable to provide the number of transactions agreed after criminal proceedings had begun.

660. The use of such transactions compensates for the limited resources allocated to the judicial system and allows decisions to be reached more quickly than when cases are referred to the courts. However, this approach to dealing with ML cases raises a number of questions of principle, as these transactions do not involve an admission of guilt or result in a conviction. Only extended agreement are entered in defendants' criminal records, but extracts from these records are only accessible to the judicial authorities and the police.

661. Furthermore, the option of resorting to such transactions even when the case has already been referred to a trial judge is no longer justified at this point in the proceedings in terms of usefulness and savings in investigative resources. The use of these transactions also raises a problem regarding its deterrent effect, as the terms of the agreement are not made public except during the public hearing at which the trial judge approves it. A judge does check to some extent that the amounts proposed in the transaction are sufficient, but only when such transactions takes place after the defendants have been charged.

662. One court has already refused to approve a transaction agreement on the grounds that the measures proposed by the Federal Prosecutor were not proportionate to the seriousness of the offences and did not act as a deterrent, as the agreement did not require the defendant to pay any money, even though their motive for committing the offences was financial.

663. The arrangements for using this non-trial resolution mechanism also raise questions about its use as an alternative means of settling ML cases. The increase in the use of the transaction procedure raises concerns that this mechanism may become a preferred means of settling ML cases and, ultimately, replace court proceedings, without the specific circumstances of the case justifying this.

[191] Circular COL 08/2018

[192] Where the prosecutor considers that the offence does not appear to be of a nature that would warrant a custodial sentence of more than two years or a more severe penalty, and where it does not involve serious bodily harm.

8 Confiscation

The relevant Immediate Outcome considered and assessed in this chapter is IO.8. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 32 and elements of R. 15, 30, 31, 37, 38 and 40.[193]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) Belgium has a comprehensive legal framework for seizure. Instructions issued by law enforcement agencies emphasise the importance of seizing criminal assets with a view to confiscating them. However, the AML action plan adopted in March 2024 does not give sufficient priority, in either a practical or ambitious way, to confiscation and does not provide the resources and training needed to effectively implement measures to identify and freeze assets in financial investigations.

b) Belgium is making increasing use of financial investigations to identify and confiscate criminal property and assets, but this is still insufficient given the country's ML risk profile. The results of seizures and confiscations are therefore not fully aligned with the stated intention to prioritise the recovery of criminal assets. They are also only partially aligned with the main sources of ML risk to which the country is exposed. With regard to TF, confiscations are more appropriately aligned with the risks identified.

c) The lack of police resources impacts the authorities' ability to conduct financial investigations and causes them to prioritise the prosecution of predicate offences rather than ML, with the result that criminals continue to benefit from the illegal financial gains derived from ML offences.

d) The Central Office for Seizure and Confiscation (OCSC) supports the prosecution authorities in managing seized assets and cooperating with foreign authorities. The authorities have a proactive policy of identifying assets located abroad, which account for a significant proportion of illegal capital flows from ML, and of enforcing confiscation orders issued by Belgian courts abroad. They have recently taken steps to overcome obstacles to international cooperation (see IO.2). However, Belgium has not sufficiently demonstrated its ability to confiscate assets and property located abroad that are derived from the laundering of predicate offences committed in whole or in part in Belgium.

e) There is no guidance for investigators and prosecutors on identifying and quantifying the value of illegal assets generated by ML that would make seizures and confiscation in ML cases more effective. Confiscations requested by the Prosecutor's Office are mostly limited to the value of

[193] Recommendations 1, 4, 15, 31, 38 and 40 are under review, see Technical Compliance Annex.

the laundered assets and the amounts are frequently reduced by trial judges, which means that criminals are not completely deprived of the profits generated by ML offences. The enforcement of confiscation measures without prior seizure takes several years and is only partially successful. In addition, the option of using criminal enforcement investigations to recover confiscated assets is an important tool but is rarely used due to insufficient resources.

f) The national ML risk analysis identifies cross-border movements of cash and bearer negotiable instruments (BNIs) as one of the main ML risk factors in Belgium (see IO.1). The authorities mainly monitor accompanied cash transport to and from non-EU countries at airports, which has led to the detection of a relatively large number of breaches of reporting requirements. However, the monitoring of intra-EU cross-border cash movements is limited, despite the high risks associated with cross-border cash trafficking. The authorities do not monitor unaccompanied cash movements passing through major logistics hubs, including the port of Antwerp. The sanctions for breaches of reporting requirements are also not a strong deterrent. These factors make Belgium particularly vulnerable, especially since the main ML schemes involve the widespread use of cash of unlawful origin.

g) The lack of a strategic approach to monitoring cash movements, particularly within the EU and linked to transit through the port of Antwerp, prevents Belgium from targeting the main sources of these flows and from confiscating assets commensurate with the identified risks to which Belgium is exposed.

h) The amounts retained by the Belgian customs authorities for infringements of the obligation to report movements of non-EU funds are relatively high but do not result in a sufficient number of confiscations. The amount of money withheld in connection with intra-EU movements is low given the high risk of cash-related ML and the high threat of drug trafficking to which Belgium is exposed. The confiscation of cash and BNI movements is used to a limited extent to identify potential cases of ML or TF, as customs authorities do not report a significant number of suspicious ML/TF transactions to prosecutor's offices. An isolated case of non-compliance with the reporting obligation led to large-scale confiscations, and this approach should be more systematically applied.

Key Recommended Actions (KRAs)

Belgium should:

a) Apply a criminal justice policy that prioritises financial investigations in ML cases with high recovery potential, even where the assets are not immediately available and accessible assets at the start of the investigation, in line with the ML risks identified in the country.

b) Allocate the necessary human and technological resources to law enforcement authorities, prosecutors, and the OCSC, so that they can conduct more systematic and thorough financial investigations and enforcement investigations in criminal cases ("enquête pénale d'exécution") and effectively confiscate criminal assets, including in complex ML/TF cases with a transnational dimension and/or involving virtual assets.

c) Implement a strategic approach, backed by the necessary resources, to target to target customs controls of accompanied and unaccompanied movements of cash and BNIs more effectively and to use information from customs and police authorities on cross-border cash transport more strategically, with a view to obtaining confiscations results commensurate with the identified risks of cash trafficking to which Belgium is exposed.

Other Recommended Actions

Belgium should:

a) Strengthen the ability of investigators, prosecutors and investigating judges to handle financial investigations in complex ML cases through regular operational training and guidance on seizure procedures and techniques, including for virtual assets, so that confiscation measures more in line with Belgium's risk profile can be imposed.

b) Strengthen the Belgian system for identifying criminal assets in foreign countries and use all available means, including diplomatic channels, to facilitate the enforcement outside Belgium of confiscation orders issued by Belgian courts.

c) Take the necessary legal measures to allow for confiscation measures without prior criminal conviction.

d) Raise the level of sanctions for failure to comply with declaration/reporting obligations for cross-border cash transport.

e) Implement legislative and regulatory requirements for keeping statistics on seizures and confiscations in ML/TF cases so that Belgium has the quantitative information it needs to implement an effective asset recovery policy (see TC Annex, R. 33).

Overall Conclusions on IO.8

Belgium has a comprehensive legal framework for seizure and confiscation. However, the country only deprives criminals of the proceeds and instrumentalities of crime to a limited extent. Although financial investigations are conducted more frequently, Belgium does not yet make sufficient use of these investigations to identify and seize criminal property and assets. The lack of resources and shortcomings in the judicial response described under IO.7 have a direct impact on the ability of the Belgian authorities to deprive criminals of illicit financial gains to the extent commensurate with the risks to which Belgium is exposed. The results of confiscations are not commensurate with national policies and priorities on AML/CFT, asset recovery and Belgium's risk profile.

There are also significant weaknesses in the system for monitoring cross-border movements of accompanied and unaccompanied cash and BNIs, particularly within the EU and at logistics hubs. The sanctions applied in the event of non-compliance do not have a significant deterrent effect. The confiscation of cash and BNI movements is used to a limited extent to identify potential cases of ML or TF. These shortcomings are all the more critical given Belgium's unique position as a strategic economic hub within Europe, the key role played by the port of Antwerp, and the fact that the authorities have identified cash flows linked to international cash trafficking as a key ML indicator. Major improvements are required.

Belgium is rated as having a Moderate level of effectiveness for IO.8.

Immediate Outcome 8

664. The evaluation team has based its conclusions on the information provided by Belgium, the analyses of available statistics and the sample of cases submitted by Belgium, as well as on discussions with various authorities, in particular the Central Office for Seizure and Confiscation (OCSC) and the judicial and investigative authorities.

665. The evaluation team encountered difficulties in obtaining certain statistical data, despite the FATF's recommendation in its 2015 evaluation report to keep centralised statistics on asset seizures and confiscations in Belgium and abroad.[194]

8.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

666. Asset recovery was identified as a priority by the authorities at the time of the FATF's 2015 report. Instructions issued since then by law enforcement agencies confirm the importance placed on seizing and confiscating criminal assets . The Federal Judicial Police's 2022 Internal Directive recommends an approach focused on 'the spoils' ('take the money') and sets out a three-pronged strategy: strengthening police training, putting in place a more systematic structure of investigation teams dedicated to tracing illegally acquired assets (PLUK teams) and increasing the number of criminal investigations to recover confiscated assets ("*enquête pénale d'éxécution*"). The ability to recover assets is the central element to decide whether to open and conduct ML investigations, following the criminal justice policy guidelines issued by the College of Prosecutors General in the TRIM circular in 2022. However, in practice, Belgium often takes a narrow approach, focusing on the seizure and confiscation of assets and valuables that are immediately available (see IO.7).

667. Furthermore, the priority given to confiscation is not sufficiently supported at a higher level by the AML action plan adopted in March 2024, which merely reiterates the importance of applying the TRIM criteria *'in view of Belgium's evaluation by the FATF'*. In addition, these guidelines have not been accompanied by additional resources for law enforcement authorities, which continue to face insufficient police resources to conduct financial investigations (see IO.7). The February 2025 government agreement contains a number of points relating to asset recovery.[195]

8.2. Confiscation of proceeds instrumentalities and property of equivalent value from foreign and domestic predicates, and proceeds located abroad

8.2.1. Identification of property and assets liable to seizure

668. In the 2015 MER, the FATF noted that Belgium needed to conduct financial investigations in a more systematic way. Since then, financial investigations have been carried out more frequently, but not yet sufficiently given the country's risks exposure. Law enforcement agencies have highlighted that, since 2015, there has been a better understanding of the importance of provisional seizing of assets and therefore of conducting financial investigations. Since 2022, the Federal Judicial Police Directorate-General has recommended that 'asset investigation teams' (PLUK teams) be set up in each FJP unit to work with investigators on the financial aspects of investigations. These teams, which already existed in seven units,

[194] There are legal and regulatory requirements for keeping these statistics in Belgium, but they have not been fully implemented (see TC Annex, R 33).

[195] Instructor's Statement 2025–2029.

including the Brussels and Antwerp FJP units, have been set up in the remaining units as of 2025.[196] Across Belgium, a total of 66 financial investigators are assigned to these PLUK asset investigation teams. The 2022 FJP Directive recommends that investigators draw up an investigative plan with prosecutors to determine the necessary measures for recovering illegal assets. This is a step in the right direction but has not yet been fully implemented in practice. The Federal Judicial Police stressed the importance of this change in approach, given that most investigations have so far focused on the predicate offences, without giving adequate consideration to the illicit assets laundered (see IO.7).

669. The way in which *financial investigations* are conducted varies from one prosecutor's office to another. They may be conducted separately from the investigation into the predicate offences or as part of a single investigation. Illicit assets located in Belgium are identified through several channels, including the central register for financial accounts and contracts (PCC – see IO.5), the Banque Carrefour des Entreprises database, the register of ultimate beneficial owners (UBOs), and the *JustBan* register of professional bans (see IO.5). Law enforcement authorities also have access to data held by the CTIF via liaison magistrates and the FJP officers seconded to it (see IO.6) and, to a limited extent, to tax and asset information held by SPF Finance and information held by the social security inspection services. The land registry, requests for banking information and searches are other channels for identifying illegal assets.

670. The Belgian authorities are also trying to determine whether it is possible to seize assets located abroad and are doing so with the help of their foreign counterparts through informal contacts arranged by the OCSC, which activates the ARO/CARIN networks (see section 8.2).

671. With regard to ML, identifying and recovering assets is central to the TRIM criteria that have guided the opening and handling of investigations since the end of 2022 (see IO.7). Criterion *R, recoup,* aims to assess the potential for recovering property or financial assets that could be confiscated. In practice, the authorities apply this criterion in a narrow way and start an investigation based on a criterion of profitability if they believe that they can immediately seize available and accessible assets during the initial stages of processing a case. In practice, seizures are mainly limited to the proceeds of the predicate offence (e.g. the resale price of cocaine in relation to the quantities trafficked, amounts evaded in social security fraud) and do not extend to funds already laundered and proceeds generated by ML activities. In ML cases involving criminal organisations, only cash constituting the network's 'cash float' is seized; cash that has already been laundered in Belgium or transferred abroad is not being adequately pursued by the authorities. The "*auditorat du travail*", responsible for social security frauds, highlighted that there is little point in prosecuting ML offences in the social fraud cases they handle, as ML does not make it any easier to obtain confiscation orders. A similar observation was made by the authorities in relation to drug trafficking. Furthermore, the high rate of cases being closed for discretionary reasons (lack of police resources) means that the potential for recovering illegal assets in some cases is not fully considered without in-depth financial investigations (see IO.7).

672. There is no guidance for investigators and prosecutors on identifying assets and on seizing and confiscating ML proceeds. Since 2022, the FJP has introduced training to familiarise financial investigators and judicial officers with the legal framework applicable for ML and with some seizure practices (e.g. virtual assets). The operational and practical aspects are not yet sufficiently covered in these trainings.

8.2.2. Provisional measures

673. *Urgent precautionary freezing* – The Belgian legal system allows for an urgent request for precautionary freezing of a transaction even before a criminal investigation has been opened (Art. 80 of

[196] The FJP units in the districts of Luxembourg, Halle Vilvoorde, Walloon Brabant, Charleroi, Eupen, Namur and Mons.

the AML Law). The CTIF has the right to object to the execution of financial transactions reported by reporting entities and any related transactions for a period of five working days. [197]

Box 8.1. Example of urgent precautionary freezing due to suspected ML

In a case involving suspected ML from organised crime, tax and social fraud, the CTIF froze the account balance of an entity suspected of being a shell company used in a case involving Brazilian networks, which stood at more than EUR 50,000, which was then paid to the tax authorities. An investigation is currently being conducted at the Brussels prosecutor's office.

674. At the beginning of 2022, the CTIF simplified the procedures for urgent request for precautionary measure to process requests more efficiently. The CTIF also used this urgent freezing procedure on its own initiative as part of a project to analyse the data available to it in order to dismantle the networks involved in ML cases related to offsetting schemes (see IO.1).

675. The number of transactions subject to urgent request for precautionary freezing is growing, from 29 transactions in 2019 to 110 transactions in 2024 (see table 8.1). These measures are a useful tool, although the Belgian authorities do not provide any details on the extent to which they subsequently lead to the seizure and confiscation of illegal assets. Their effectiveness is also increasingly being challenged by advances in payment technologies, such as instant and electronic payments, which shorten the time available to take action. In addition, the targeted bank accounts are often used as transit accounts, with balances that tend to be kept low, making it more difficult to effectively implement measures to prevent transactions and seize assets.

Table 8.1. Urgent requests for precautionary freezing ordered by the CTIF

	2019	2020	2021	2022	2023	2024	Total
Amount (EUR millions)	3.77	30.58	7.04	4.72	4.49	9.63	60.23
No. of transactions	26	33	44	56	62	110	331

Source: CTIF

676. *Seizures* – Belgium has a comprehensive legal framework for seizures, which can be ordered directly by prosecutors and investigating judges without prior authorisation from a judge. Seizures were used in an increasing number of ML cases over the period from 2019 to 2024 (see table below), including for large amounts. Assets worth approximately EUR 30 million were seized. Approximately one quarter to one third of the amounts seized and managed by the OCSC were in 5 681 cases involving suspected ML totalling nearly EUR 166 million. However, Belgium often takes an approach that is still too limited, focusing on the seizure of assets and valuables that are immediately available (see IO.7).

Table 8.2. Total sums seized for predicate offences, ML and TF (EUR million)

	2019	2020	2021	2022	2023	2024 (est)	Total
All offences	93	108.2	104.7	114.9	109.8	110.3	**640.9**
Drug trafficking	8.8	15.9	14.2	11.7	12.8	15.390	**78.81**
Tax fraud	2.3	9	3.5	2.2	3.2	5.618	**25.81**
Social fraud	5.28	3.72	12.13	5.53	6.65	6.31	**39.62**

[197] In the case of a transaction reported by an obliged entity or identified in a suspicious transaction report or a request for assistance from a foreign FIU. The period may be extended beyond five days, in which case the CTIF must inform the public prosecutor or the federal prosecutor.

	2019	2020	2021	2022	2023	2024 (est)	Total
Scam	5.7	4.6	4.5	6.6	7.6	9.985	**39.02**
Organised crime	13.5	6.5	11.2	12.8	15	13.392	**72.43**
ML	22.7	21.6	31.5	22.7	27.3	39.6	**165.66**
TF	0.014	0.265	0.071	0.007	0.017	0.004	**0.378**

Note: These amounts correspond to the sums seized and managed by the OCSC. Due to a file coding procedure, some sums seized in relation to ML may not have been coded.
Source: OCSC statistical data

Table 8.3. Total value of assets in kind seized and managed by the OCSC for ML/TF

	2019	2020	2021	2022	2023	2024 (est)	Total
Seized (ML)	5 120 147	160 125	1 018 512	3 850 479	18812579	1464134	30425975
Investigations	9	4	6	9	14	10	52
Seized (TF)	0	0	0	0	0	0	0

Source: OCSC statistical data

677. The Sky ECC case led to a significant number of seizures by the Belgian authorities, including abroad (totalling approximately EUR 215 million), some of which were in ML cases that resulted in confiscation. Nevertheless, the overall volume of seizures in Belgium did not increase significantly, due to resource constraints on the police, who had to limit seizures in other cases.

678. The total amount seized in ML cases appears limited overall given the country's risk profile, dominated by organised crime and significant exposure to drug trafficking and social and tax fraud, generating substantial illegal proceeds, some of which are laundered in Belgium. The Belgian authorities explain that the limited number of seizures in ML cases is due to the difficulties involved in locating assets outside Belgium, as Belgium would be mainly as a transit country. This raises questions about the proactive nature and timing of the measures taken by the Belgian authorities to curb the movement of illegal assets out of Belgium and the flow of illegal funds remaining in Belgium, for example in the case of polycriminal ML activities involving offsetting schemes (see IO.7).

679. In terms of TF, the value of seizures handled by the OCSC is relatively low but appears consistent with the country's risk profile, characterised in particular by microfinance (see table above and IO.1 and 9). Over the period from 2019 to 2024, seizures totalling EUR 378 000 were made in 27 TF cases.

680. Analysis of data decrypted in the Sky ECC case revealed a growing use of virtual assets by criminals. The Belgian authorities have demonstrated that they are capable of seizing virtual assets. Between 2019 and 2024, a total of almost EUR 28 million in virtual currency was seized across 59 investigation files covering all offences, including EUR 20 million in 48 ML investigations. These seizures were made possible by the existence of specialised officers within the FJP who are skilled in specific types of analytical work. The Belgian authorities explain that seizures and confiscations of virtual currency have been limited in ML/TF cases due to their complexity, which requires longer judicial proceedings.

Table 8.4. Seizure of virtual assets in ML/TF cases

	2019	2020	2021	2022	2023	2024 (est)	Total
Total virtual assets (EUR)	261 337	37 393	3 607 359	1 936 615	7 439 589	7 067 000	20 349 293
No. ML files	0	0	0	43	4	0	47
Total virtual assets (EUR)	0	0	0	0	0	8 737	8 737
No. TF files	0	0	0	0	0	1	1

Source: OCSC statistical data

8.2.3. Asset management by the OCSC

681. The OCSC manages seized assets in a relatively effective manner. It sells certain seized assets prior to judgement to avoid depreciation. A pre-judgement sale results in the funds being deposited in the OCSC's account for the duration of the proceedings. Between 2019 and 2023, disposal decisions were taken in 4 305 court cases involving vehicles. These were sold through Fin Shops for a total of EUR 20.88 million. In addition, the OCSC has set up special mechanisms for managing virtual assets (see box below).

Box 8.2. Example illustrating the capability to seize and manage virtual assets

In a case involving drugs and criminal conspiracy, significant seizures were made including cash, luxury watches, sports cars and virtual assets. An initial seizure of approximately EUR 6.5 million in virtual assets was made in October 2023 on an exchange platform. The seizure and management of the seized assets took place as part of a public-private partnership set up by the OCSC, with the police automatically creating different virtual asset portfolios for each seizure on the various platforms. The seizure was therefore effective as soon as the assets were transferred to accounts opened with the OCSC's private partner. The seized assets could then be managed directly via the platform. Consequently, the OCSC sold part of the seized virtual assets for EUR 2.2 million. A new seizure was carried out in September 2024. The OCSC still manages virtual assets worth EUR 6.3 million.

8.2.4. Confiscation and enforcement of confiscation orders

682. Belgium has a legal framework that allows assets to be confiscated where no lawful origin can be established,[198] which should make it easier to confiscate proceeds, instrumentalities of crime or property of equivalent value (see TC Annex, R 4). Belgian case law considers that property obtained through money laundering constitutes a financial gain derived from that transaction and may be subject to confiscation.[199] Confiscations have been ordered following convictions *in absentia*, as well as in cases where sentencing has been deferred or a simple conviction has been handed down.

683. However, Belgium cannot enforce confiscation measures without a prior conviction, even at the request of foreign authorities, as Belgian law does not provide for this possibility.[200] In the case of a transaction procedure, Belgian law provides for the voluntary surrender of property or financial gains, whether seized or not, by the perpetrator of offences that may give rise to confiscation. Belgium does not provide the amounts that have been recovered in this way.

684. In ML cases, the evaluation team found, based on the case examples provided by Belgium, that the prosecutors' indictments tend to be limited to confiscating the value of the laundered property, without quantifying the proceeds obtained through ML. The confiscation amounts imposed therefore represent only part of the benefits derived from ML. Prosecutors also reported frequent reductions in the confiscation amounts requested by trial judges. Judges have full discretion to assess the impact of confiscation measures so as not to impose an unreasonably heavy sentence on the convicted person (pursuant to Article 505(6) and (7) of the Penal Code). The amounts to be confiscated can also be reduced when judges consider that judicial treatment of cases exceeded a reasonable time limit. Judges have applied this reduction in the

[198] Cass., 21 March 2006, RG no. P.06.0034.N, Pas., 2006, 165; Cass., 12 June 2013, RG no. P.13.0312.F, Pas. 2013, 363; Cass., 5 February 2019, RG no. P.18.1010.N

[199] Cass., 10 September 2024, RG no. P.14.0475.F/3

[200] A bill is currently being drafted to transpose Directive 2024/1260 of the European Parliament and of the Council into Belgian law.

amounts to be confiscated even in cases of money laundering involving multiple offences committed by complex and organised networks. The 'Clown' case is one example (see box under IO.7).

685. The number of ML cases in which confiscations are ordered is rising, but the average value of the amounts confiscated remains relatively stable overall. This finding is based on partial statistical data provided by the OCSC on amounts confiscated following provisional seizures. Belgium has provided examples of ML cases demonstrating its ability to confiscate significant amounts. Between 2019 and 2024, EUR 39.5 million was confiscated in ML cases following prior seizures (see table below). These amounts demonstrate Belgium's ability to strip criminals, to a certain extent, of assets obtained illegally through ML schemes. However, these amounts remain relatively low given Belgium's context and risk profile (see IO.1). The amount of equivalent-value confiscations ordered without provisional seizures in ML/TF cases is not known.

Table 8.5. Amounts confiscated for all offences and ML

	2019	2020	2021	2022	2023	2024 (est)	Total
ML* (EUR millions)	8.4	2.8	3.6	4	7.3	13.1	39.7
No. of files	198	180	244	267	340	119	1 348
All offences**							
Amounts of equivalent-value confiscations (sums and real estate)	241.2	236.5	216.19	319.9	547.7	509.3	2 070.79
Recovery rate of amounts confiscated (January 2025)	26.5%	32%	26.11%	13.87%	20%	10.43%	19.4%
Amounts confiscated as a result of seizures managed by the OCSC	22.4	11.5	18.9	19.7	28	39.4	139.9

Note: These figures do not include amounts of equivalent-value confiscations without prior seizure that are not managed by the OCSC, nor amounts confiscated in cases opened for offences other than money laundering but resulting in convictions for money laundering.

*The amounts include all assets seized prior to judgement (i.e. sold during the investigation of seized assets so that the cash proceeds could replace the original seized assets) and confiscated, in addition to the sums confiscated. Confiscated assets in kind that were not seized or disposed of prior to judgement are not included.

**This includes all sums and the equivalent value of confiscated real estate managed by the OCSC, without details of the offences concerned being known.

Source: OCSC

686. In terms of TF, the authorities confiscated a total of EUR 753 191 between 2019 and 2024 in eight cases. Although these figures are much lower than those for ML, they are in line with the number of TF cases opened and the TF typology, which since 2016 has mainly involved microfinance transactions (see IO.1 and IO.9).

Table 8.6. Amounts confiscated for TF offences

	2019	2020	2021	2022	2023	2024 (est)	Total
Confiscation (EUR)	0	6 530	10 365	0	33 880	702 416	753 191
No. of files	0	1	2	0	2	3	8

Note: These figures do not include amounts of equivalent-value confiscations without prior seizure that are not managed by the OCSC.

Source: OCSC

687. *Equivalent-value confiscations* – Where prior seizures have not been possible, Belgium may resort to equivalent-value confiscation measures.[201] However, equivalent-value confiscation is only effective if it is supported by an effective asset recovery system, which is not the case in Belgium. During the period

[201] This is a sentence to pay a sum of money equivalent to the benefits derived from committing the offence and not found in the convicted person's assets.

under review, Belgian courts ordered a total of EUR 2.07 billion in equivalent-value confiscations across all offences. However, there are significant difficulties in enforcing confiscation measures (see below). Belgium does not have more detailed data on the amounts of equivalent-value confiscations for each predicate offence and for ML/TF. However, examples provided to the evaluation team demonstrate that Belgium is able to order equivalent-value confiscations for significant amounts in ML cases.

Box 8.3. Equivalent-value confiscation in an ML case involving international drug trafficking

In an ML case involving international drug trafficking by a criminal organisation, the judicial authorities seized a total of more than EUR 4 million. The court ordered the confiscation of an equivalent value totalling EUR 89 million from 13 defendants. Furthermore, in the same case, a confiscation order for an equivalent value of EUR 7.6 million was handed down against a defaulting party.[202]

688. *Additional confiscation measures* – The Belgian authorities almost never make use of the option of imposing additional confiscation measures provided for in the Penal Code (Art. 43 quater, para. 2 and 3). These measures allow for extended confiscation orders to be imposed where the authorities find that the accused's assets have increased and there are serious and substantive indications that this increase is the result of the offence for which they have been convicted. The authorities have stated that this legal option has only been used twice in connection with convictions for drug trafficking.

689. *Enforcement* – There are significant difficulties in enforcing confiscation measures. In total, Belgium has recovered less than one fifth (19.4%) of the amounts for which equivalent-value confiscation ordered between 2019 and 2024.[203] This low recovery rate is mainly due to the insufficient resources allocated to law enforcement agencies to identify and trace illegal assets. Belgium has the option of initiating a criminal investigation to enforce confiscation measures following a conviction and recover assets *("enquête pénale d'exécution")*. This investigation can be conducted by prosecutors with the support of the OCSC or delegated to the OCSC. The authorities have similar investigative powers to those available in regular criminal investigations. These investigations are a useful process to enforce confiscation measures, provided sufficient resources are available for their conduct. However, the same resource constraints apply for those criminal investigations. The authorities have indicated that approximately 150 cases per year lead to the opening of a criminal investigation to recover assets.

690. However, the results of these criminal investigations are not evidenced in the recovery rates, which remain low and are only marginally improving. Only 26.5% of the amounts confiscated in 2019 had actually been recovered by January 2025.

8.2.5. Confiscation of crime proceeds located abroad

691. The OCSC plays an active role in the identification and tracing of criminal assets located abroad. by using informal cooperation through the ARO and CARIN networks. It centralises and sends requests for mutual assistance abroad to support the needs of investigations in Belgium. Overall, incoming and outgoing requests for information relating to tracing, identifying and seizing proceeds of crime are increasing. Between 2019 and 2023, the OCSC sent a total of 1 586 requests abroad and received 1 115 requests from abroad through the ARIN/CARIN networks, across all offences. Between 2020 and 2024, the OCSC sent 584 requests abroad to identify property in ML cases. In 2023, the main partners were the

[202] Judgement of 27 April 2022 of the Brussels Criminal Court pursuant to Article 505 6° of the Penal Code.

[203] These figures do not include confiscations in kind of movable and immovable property, which are mostly ordered on property that has been previously seized.

Netherlands, Spain and France. During the same period, Belgium processed 483 ML-related requests from abroad, mainly from Germany, the Netherlands and France. The number of requests received suggests that Belgium is not only a transit country.

692. Belgium does not provide detailed information on the results of these requests, whether incoming or outgoing., It indicates that requests related to the identification of bank accounts (Belgium has authorised the sharing of bank information through the ARO/CARIN networks since September 2022) and real estate have led to formal requests for mutual assistance from the judicial authorities of the countries concerned for the purpose of seizing these assets. For example, in 2023, out of 447 outgoing requests, 301 led to the identification of assets abroad and the remaining 146 were unsuccessful.

693. The Belgian authorities are faced with difficulties in seizing assets located outside the EU, which require lengthy international cooperation measures that sometimes lead to results that are sometimes random. For some prosecutor's offices, these difficulties are a reason for not launching investigations in Belgium and, in some cases, preferring to report the offences to competent foreign authorities ("dénonciations", see IO.2).

694. Belgium pursues a proactive policy to enforce equivalent-value confiscation orders issued by Belgian courts abroad. However, the authorities face significant obstacles in certain countries of origin of suspects or countries that serve as safe havens outside the EU (i.e. Albania, Brazil, the United Arab Emirates (UAE), Morocco and Turkey). The Belgian authorities are taking steps to build closer ties with these countries. For example, Belgium has signed a judicial cooperation agreement with the UAE and appointed a specialist prosecutor to the Federal Prosecutor's Office. It has seconded a liaison prosecutor to Morocco and is seeking to establish direct relations, which are sometimes hampered by diplomatic setbacks. Recent results have been encouraging and need to be sustained (see IO.2). Given the importance of equivalent-value confiscations of assets located abroad, strengthening the system for identifying criminals' assets abroad and enforcing court decisions is of strategic importance for Belgium. However, Belgium does not have statistics on the enforcement of confiscation orders abroad and has not provided examples of cases that clearly demonstrate its effectiveness.

Table 8.7. Requests issued by the OCSC (ML case)

	2019	2020	2021	2022	2023	2024	Total
No. of ARO/CARIN mutual legal assistance requests in open ML cases	56	69	62	93	136	168	584
Total ARO/CARIN requests	251	249	299	340	447	620*	2206

Note: *For 2024, out of 620 outgoing requests (ARO and CARIN), 351 requests were made in connection with the enforcement of equivalent-value confiscations ordered by Belgian courts.
Source: OCSC statistical data

8.2.6. Repatriation, sharing and restitution

695. With regard to sharing confiscated assets and property with the countries concerned, cooperation with EU countries takes place at the level of the competent judicial authorities, and the legal framework provides that where the amount confiscated exceeds EUR 10 000, the proceeds are shared equally between the enforcing State and the issuing State (Art. 38 of the law of 5 August 2006 and European regulations). Different sharing arrangements may be agreed on a case-by-case basis, and these must be formalised in a bilateral agreement between the Ministers of Justice. Outside the EU, sharing confiscated assets and property is governed by various international conventions and by the Law of 20 May 1997 (see TC Annex, R 38). In practice, SPF Justice, the judicial authorities and the OCSC work together and decide on a case-by-case basis whether sharing the property is appropriate.

8.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI

696. Belgium has a legal framework based on the European framework supporting the obligation to declare cross-border movements of cash and bearer negotiable instruments (BNIs) outside the EU. Failure to comply with this obligation is a customs offence and is enforced by the Belgian customs authorities. Belgium has adopted national provisions governing intra-EU cross-border transports, which are enforced by customs and the police (see TC Annex, R 32).

8.3.1. Identification and confiscation of cross-border movements of cash and bearer negotiable instruments that are falsely declared/undeclared

697. The ML NRA identifies international trafficking in cash as a major risk for Belgium (see IO.1). However, the risk of unaccompanied transport of cash and BNIs, including through the port of Antwerp, is not taken into account in the implementation of checks on cross-border movements of cash and BNI.

698. *Checks on flows outside the EU* – Customs checks on cash movements and BNIs outside the EU are based on the results of supranational risk assessments carried out by the European Commission (most recently in October 2022). Belgium has not developed its own criteria and follows the common criteria established at European level. However, Belgium's specific context and the position of the port of Antwerp as a major gateway to the EU call for Belgium to develop specific criteria. At present, the authorities carry out checks on cash accompanied to and from non-EU countries at Brussels-Zaventem and Charleroi-Gosselies international airports, but these are not carried out in a sufficiently targeted manner. The Belgian Passenger Information Unit (BelPIU) database, which collects and analyses data on passengers travelling internationally to, from or through Belgium, cannot be used to target customs checks on cash and BNI movements.[204]

699. Customs officers were nevertheless able to detect a relatively high number of breaches (see table below). Between 2021 and 2024, they recorded a total of 4 291 declarations involving a total of EUR98.8 million. During the same period, customs authorities identified 1888 offences involving a total of EUR28.1 million. At Brussels Midi international railway station, a total of EUR 1.8 million was seized by the Belgian Railway Police between 2021 and 2024. However, Belgium has not provided the total amounts seized and confiscated, nor any information on any legal action taken in relation to these offences.

Table 8.8. Number of declarations and offences detected (2021–2024) outside the EU

	2021*		2022		2023		2024	
	Declarations	Offences	Declarations	Offences	Declarations	Offences	Declarations	Offences
Total airports	497	308	1 282	721	1 125	597	537	257
Total international station (Brussels)	4	1	9	1	5	3	0	0
Total ships' crew cash	137	0	226	0	311	0	152	0
Other (public roads/parcels)	0	0	3	0	3	0	0	0
TOTAL	**638**	**309**	**1 520**	**722**	**1 444**	**600**	**689**	**257**

[204] Regulation (EU) 2025/13 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818.

	2021*		2022		2023		2024	
Total (EUR millions)[205]	**14.4**	**5.3**	**34.2**	**10.6**	**33.8**	**8.5**	**16.4**	**3.7**

Note: *Data for the period from 03/06/2021 (entry into force of the new Regulation 2018/1672) to 31/12/2021.
Source: Customs data on declarations and offences relating to movements of funds outside the EU. Last updated on 10 June 2024.

700. *Checks on intra-EU flows* – Checks carried out by customs authorities and the police on cross-border movements of funds and BNI within the EU led to identifying a limited number of falsely declared or undeclared movements of cash and BNIs. Between 2021 and 2024, 342 disclosures of funds transported exceeding EUR10,000 were recorded, involving a total of EUR9 million. During the same period, customs authorities detected 60 offences involving a total of EUR1.1 million (see table 8.8 below). Confiscations obtained as a result are not known. These amounts are low given the high risk of cash-related ML and the high threat of drug trafficking to which Belgium is exposed. They also raise questions about the effectiveness of customs and police checks at Belgium's land borders, as the Belgian authorities suspect organised criminal groups of repatriating, by land and through countries bordering Belgium, some of the illegal proceeds that are then transferred out of the EU to their members' countries of origin (e.g. Albania, Turkey) via low-level couriers. Given Belgium's risks in terms of cash laundering, the lack of a national strategy for intra-EU border checks tailored to the particular characteristics of the Belgian context is penalising.

Table 8.9. Number of declarations and offences detected (2021–2024) within the EU

	2021		2022		2023		2024	
	Declarations	**Offences**	**Declarations**	**Offences**	**Declarations**	**Offences**	**Declarations**	**Offences**
Total airports	11	1	41	1	68	30	43	28
Total international station (Brussels)	3	0	2	0	0	0	0	0
Total ships' crew cash	25	0	47	0	67	0	28	0
Other (public roads/parcels)	0	0	5	0	2	0	0	0
TOTAL	**39**	**1**	**95**	**1**	**137**	**30**	**71**	**28**
Amount (EUR millions)[206]	0.9	0	2.8	0	3.6	0.5	1.7	0.6

Source: Customs data on declarations and offences relating to movements of funds within the EU. Last updated on 10 June 2024.

701. *Unaccompanied cash and BNIs* – Belgium has set up systems to detect illegal goods (drugs, weapons, protected species, counterfeit goods, etc.) at its main logistics hubs (airports and freight ports), but there are no specific checks on cross-border movements of unaccompanied cash and BNIs upon leaving the country, which is a weakness in the system. In any case, the checks carried out are not adequate for identifying movements of unaccompanied cash and BNIs. Belgium has not provided figures on the number of customs offences identified and amounts seized in connection with the transport of unaccompanied cash and BNIs (by air freight, cargo freight or land courier).

[205] The largest customs seizures recorded between June 2021 and June 2024 at Zaventem International Airport amounted to between €102,300 and €609,975 and involved cash exports to Turkey, China and the UAE, and cash imports from the Democratic Republic of Congo, Israel and Thailand.
[206] The largest customs seizures recorded between June 2021 and June 2024 at Zaventem International Airport amounted to between €102,300 and €609,975 and involved cash exports to Turkey, China and the UAE, and cash imports from the Democratic Republic of Congo, Israel and Thailand.

8.3.2. Confiscation of cash and negotiable bearer instruments related to ML/TF or predicate offences

702. When a customs offence is detected, the customs authorities draw up a report which is sent to the prosecutor's office. The CTIF has access to this information via the Customs Information System (CIS) database. The customs authorities also send regular reports to the prosecutor's office when no customs offence has been detected but there is a suspicion of criminal activity, even if the sums transported are below the declaration thresholds. In both cases, customs may temporarily retain the funds. The onus is on the suspect to justify the origin and destination of the funds. Between 2021 and 2024, the total amount of falsely declared or undeclared cash movements and BNIs identified by customs amounted to EUR 29.2 million. Amounts actually confiscated as a result are not known.

703. In addition, the confiscation of cash and BNI movements appears to be used to a limited extent to identify potential cases of ML or TF. The customs authorities reported a relatively low number of suspected ML/TF offences based on non-compliance with declaration or reporting requirements. Between 2019 and October 2024, they sent a total of 149 reports to prosecutor's offices for suspected ML following the discovery of customs offences relating to cash transport declarations during checks carried out at Brussels-Zaventem and Charleroi international airports. Belgium also provided examples where large sums of cash were detected in passengers' luggage, some of which were confiscated. The Halle Vilvoorde prosecutor's office opened investigations into 79 cases and closed 43 of them, i.e. more than half of the reports received. The number of ML investigations opened by the Charleroi prosecutor's office is not known. The number of cases submitted to these two prosecutor's offices each year is decreasing, from 52 in 2019 to 23 in 2021[207] and then 15 in 2024.[208]

704. However, prosecutors in some districts have indicated that they are unable to investigate all suspected offences referred to them by the customs authorities, mainly due to a lack of resources. Intelligence from customs authorities and the police on cash trafficking and ML is limited considering the level of risk in Belgium.

705. In this context, one major case stands out (see box on the Pondjes case, IO. 7). In this case, customs officials detected non-compliance with the obligation to declare cash movements, which led to the discovery of a significant money laundering network operating offsetting schemes and the confiscation of EUR 26.5 million, in addition to the undeclared cash. The significant resources deployed were crucial to the handling of this case, and the prosecutors responsible stated that they were unable to take on any more cases of this magnitude due to a lack of resources.

8.3.3. Sanctions

706. Belgium has a range of sanctions applicable to falsely declared/non-declared cross-border movements of cash and BNIs outside the EU (between EUR 125 and EUR 1 250). Taken in isolation, these amounts are not sufficiently proportionate or dissuasive in view of the amounts of undeclared cash seized that Belgium has brought to the attention of the evaluation team (see R 32). In practice, customs authorities mainly resort to out-of-court settlements for the vast majority of offences. Belgium has not provided information on the number of settlements and sanctions imposed.

[207] The introduction of the new European system for declaring cash movements, which came into force in 2021, has had an impact on the number of cash movement declarations made to customs.

[208] The statistics do not make a distinction between files referred for failure to declare and those referred for incorrect declarations. Nor is it possible to distinguish between cases relating to cross-border movements of funds within the EU and movements outside the EU.

707. Failure to comply with the obligation to declare cross-border transfers of funds within the EU does not constitute a customs offence and falls within the jurisdiction of the prosecutor's office. Belgium has not provided information demonstrating its ability to impose sanctions for such failures.

8.4. Consistency of confiscation results with ML/TF risks and national AML/TF policies and priorities

708. The confiscation results in ML cases are generally not in line with national AML and asset recovery policies and priorities. They also do not correlate with the ML risks to which Belgium is exposed. In comparison, the confiscation results in TF cases are more aligned with national TF policies and the TF risks to which Belgium is exposed.

709. The statistics available do not provide a comprehensive picture of the results obtained by type of predicate criminal offence. However, they are sufficient to establish the lack of correlation between the results of seizures and confiscations for the offences generating the highest profits in the country. The lack of police resources impacts the authorities' ability to identify and confiscate ML proceeds and to achieve results commensurate with the risks to which Belgium is exposed. As a result, criminals continue to enjoy the illicit financial gains derived from ML offences. The shortcomings in the judicial response described in IO.7 have an impact on confiscation results.

710. In light of the increased threat of ML linked to cash trafficking, seizures related to cash trafficking are not commensurate with Belgium's identified risk profile. This constitutes a significant vulnerability in the Belgian scenario, where risks associated with illegal cash flows are significant.

9 Terrorist financing investigations and prosecutions

The relevant Immediate Outcome considered and assessed in this chapter is IO.9 The Recommendations relevant for the assessment of effectiveness under this chapter are R. 5, 30, 31 and 39 and elements of R. 1, 2, 15, 32, 37 and 40.[209]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) Belgium has reassessed its response to terrorism following the terrorist attacks of 2015 and 2016 and is paying greater attention to its financing. The system in place, as well as its implementation, appear coherent and benefit from the necessary resources to detect and prosecute cases of terrorism (T) and terrorist financing (TF). Operational capacity are adequate to deal with all cases. All types of TF-related activities are investigated and prosecuted, in line with the country's TF risk profile.

b) Belgium's response to TF is based on close operational integration between measures to combat terrorism and its financing. This approach is based on a multidisciplinary approach and the centralisation of information within the framework of intelligence exchange and coordination platforms - the Joint Intelligence Centres (JICs) and Joint Decision Centres (JDCs). Initially piloted in Brussels, the JIC/JDC process was extended in 2023 to all districts of Belgium. Belgium does not have the consolidated data to accurately quantify TF cases identified through the JICs/JDCs. However, available information indicates that the JICs/JDCs have been handling all TF investigations. This approach ensures a rapid and coordinated response to all TF cases.

c) The intelligence gained from investigations into terrorism cases is used effectively to detect cases of TF, and vice versa. The information exchanged within the JICs/JDCs is centralised in the Banque de données communes (BDC) for the purposes of case tracking and the use of intelligence.

d) As things stand, the authorities do not appear to be sufficiently equipped to adapt their approach quickly to new financing methods, particularly those related to virtual assets and emerging technologies, or to strengthen the detection of informal financial networks.

[209] Recommendations 1, 2, 6, 7, 8, 14, 15, 16, 32, 38 and 40 are under review; see Technical Compliance Annex.

e) Investigative and intelligence authorities work in close and constant cooperation with the Federal Prosecutor's Office, within a structured and coordinated framework. The Federal Prosecutor's Office has a dedicated section and specialised resources appropriate to its needs. The opening and follow-up of T/TF cases are formalised and shared with all the authorities involved, including the CTIF, for example during the counter-terrorism strategy meetings (MONITOR).

f) The sanctions imposed for TF convictions are mainly prison sentences of up to five years. This sentence is often partially suspended, combined with a probation period allowing for probationary follow-up and fines. In some isolated cases, community service orders are also imposed. Overall, these sanctions are consistent and appear to be dissuasive.

g) The Prosecutor's Office sometimes uses 'judicial probation'(probation prétorienne), an alternative mechanism to prosecution, in cases where humanitarian or family considerations outweigh the prosecuting of TF. While this mechanism may be justified in certain cases, its application in TF cases, particularly when the small amounts of family money transfers are included in the decision-making criteria, raises questions of consistency with the objective of TF deterrence.

h) In some instances, notably in cases involving informal money transfer networks or when terrorist intent cannot be proven, courts resort to other classifications (violations under the law on payment institutions or AML law), either in addition to, or as an alternative to, a TF conviction.

Recommended Actions

Belgium should:

a) Institutionalise a formal follow-up and feedback mechanism for TF cases detected or reported by coordination platforms, in order to improve detection and investigation methods, share lessons learned, and disseminate best practices between departments.

b) Broaden the membership of the JICs/JDCs by involving in a more systematic way and as needed other authorities, such as the CTIF or the tax authorities, to enrich information exchange from the analysis phase onwards.

c) Revise the criteria for the use of judicial probation in TF cases to ensure consistency with the objectives of criminal deterrence.

d) Establish a mechanism to collect and centralise encrypted data on TF cases detected or investigated within the framework of JICs/JDCs, to improve statistics on investigations, prosecutions and convictions.

e) Improve the traceability of court rulings in TF matters, by strengthening the documentation on the choice of criminal classification, particularly in cases where the TF offence is not retained but replaced by alternative classifications (violations of the law on payment institutions and/or money laundering, etc.), in order to allow Belgium to better assess the effectiveness of its response to TF.

f) Consolidate operational expertise and specialisation within the relevant investigative and prosecution departments, by strengthening TF centres of expertise to ensure continuity in the processing of case.

g) Adapt skills, including technical expertise, to evolving TF threats and methods, particularly those involving virtual assets and informal financing mechanisms (e.g. hawala), to better detect and disrupt these networks.

h) Consider developing public-private partnerships on countering TF, to leverage TF detection, data processing and analysis capabilities developed in the private sector (such as digital platforms), particularly in the area of virtual assets.

Overall Conclusions on IO.9

The Belgian CFT system is based on a solid architecture combining institutional cooperation, strategic integration (especially via the JIC/JDC platforms) and judicial centralisation at the Federal Prosecutor's Office level. The criminal justice response is generally coherent: TF offences are mostly prosecuted, convictions are frequent, and the various types of threats – including micro-financing – are integrated into the operational strategy.

However, they are structural limitations to this effectiveness. Firstly, the deterrent effect of sanctions remains uneven, with some cases concluded by a suspended sentence or judicial probation, even when the facts have been established. This can in certain instances undermine the clarity of the punitive framework and weaken the preventive impact of criminal justice system, particularly in cases involving small amounts or family-related. Secondly, the level of specialisation among prosecutors and investigators still need to improve, in response to evolving, often informal TF methods, such as virtual assets and hawala-type networks.

Immediate Outcome 9 has therefore been largely achieved, supported in particular by a coherent institutional framework, specialised judicial resources and good coordination between stakeholders. However, moderate improvements are needed to enhance the criminal justice response and better address rapid developments in TF methods, particularly those involving informal channels and virtual assets.

Belgium is rated as having a Substantial level of effectiveness for IO.9.

Immediate outcome 9

711. The evaluation team has based its conclusions on a study of numerous cases showing the different types of TF, the statistics provided, the national risk analysis (NRA) and discussions with the Belgian authorities.

9.1. TF activity identified and investigated

9.1.1. Identification and investigation of TF activity

712. The detection of TF in Belgium is closely linked to efforts to counter terrorism, which reached a turning point in 2016 after the attacks in Paris (2015) and Brussels (22 March 2016). These attacks profoundly changed the country's security landscape, leading to a reorganisation of counter-terrorism strategies and, by extension, of efforts to counter TF. Since 2018/2019, the authorities have observed a change in the TF threat. Whereas terrorism previously relied on often structured and sizeable funding, it now depends on more modest and fragmented resources. The rise of isolated and/or radicalised actors has reduced the need for significant equipment funding, with attacks often carried out with limited resources (knives, vehicles, online propaganda). This shift towards more discreet and difficult-to-trace financing, particularly through the use of virtual assets, makes detection more difficult. The TF NRA partly

reflects this shift towards more diffuse forms of financing, but it remains a relatively academic exercise that does not fully reflect the operational realities observed in the field (see IO. 1).

713. Detecting TF used to rely mainly on spotting visible financial flows, such as those going through manual money changers. It has gradually become more structured to include analysing micro-transactions and spotting links between people and opaque organisations. However, a significant proportion of TF activities take place through underground or alternative channels, such as informal transfers and cash, which operate outside regulated systems. This makes detecting them more difficult, especially when banking investigations do not reveal any obvious anomalies. This structural opaqueness is a major barrier to the early detection of TF cases.

714. The CTIF identifies suspicious transactions and alerts authorities to unusual movements. The decrease in the number of CTIF reports since 2021/2022 is linked to changes in the types of TF cases and the reduced number of Foreign Terrorist Fighters (FTFs) leaving Belgium to join terrorist groups. At the height of the TF phenomenon (2017–2022), 80% of TF files were opened as a result of reports received from the CTIF, as illustrated by the Syrian Wallets case (see box 4.1).

Box 9.1. Syrian Wallets case

Background: The Syrian Wallets case is part of a structured CFT project covering the period from 2017 to 2022. It involved transfers of funds to conflict zones, mainly via money collectors based in Lebanon and Turkey. The funds originated mainly from backers located in Belgium, outside traditional banking channels. The investigation aimed to identify links between these transfers and Foreign Terrorist Fighters (FTFs) involved in the Syrian-Iraqi conflict zone.

CTIF role: (IO.6 relevance): The CTIF was asked to analyse financial flows between individuals identified as money collectors. Based on lists provided by Europol, the CTIF helped to identify additional Belgian and foreign collectors, establish links with FTFs, and identify any evidence indicating that they were still alive or might return to Belgium.

Investigation: The investigation was coordinated between the Belgian and French prosecutor's offices, involving 18 investigating judges and specialised departments of the Federal Judicial Police (organised crime and financial section). The investigation consolidated evidence gathered by the CTIF and the police, in particular through investigations into Western Union transfers and targeted phone tapping.

Outcome: The project led to the identification of numerous new money collectors, both Belgian and foreign, as well as new FTFs. It strengthened inter-agency cooperation, made it possible to link financial and judicial data, and supported several criminal proceedings.

Prosecution: Although the main case was initially closed without further action to allow for a solid case to be built (particularly after receiving the CTIF's analysis), several judicial investigations were subsequently opened based on the information provided. Prosecutions were brought pursuant to Art. 140 of the Penal Code (participation in a terrorist group).

Conviction and sanction: On 26 June 2023, the Brussels Criminal Court handed down a judgement in absentia convicting several defendants for transferring money to Islamic State fundraisers, including: 1) 10 months' imprisonment, a fine of €1,200 + €200 for the Victims' Fund; 2) 11 months' imprisonment, a fine of €1,600 + €200 for the Victims' Fund; 3) 1 year's imprisonment, a fine of €1,200 + €200 for the Victims' Fund.

715. However, the CTIF's detection of informal systems, such as hawala, remains very limited, as this system is by its very nature largely beyond the scope of conventional AML/CFT monitoring mechanisms.

These informal networks are rarely detected in Belgium, with only four cases resulting in convictions for TF through hawala. Identifying them often relies indirectly on random police checks (money mules transporting cash), ad hoc investigations (drug trafficking, etc.) or the detection of weak signals, such as repeated transfers of small amounts to at-risk areas from bank accounts with no consistent economic profile. This two-track approach to detection requires constant changes to investigation and intelligence methods to ensure that both formal and informal financial flows are covered.

Table 9.1. Number of CTIF TF reports (2019–2024)

Year	Number of CTIF reports
2020	33
2021	15
2022	22
2023	11
2024	6

716. Since 2016, numerous changes have taken place in Belgium, partly as a result of the findings of two parliamentary committees that sought to reflect on and learn lessons from the terrorist attacks of 2015 and 2016. A French report published in July 2016[210] identified flaws in cooperation between the French and Belgian intelligence services and recommended measures to improve coordination. However, it was the Belgian report of 15 June 2017[211] that marked a turning point by analysing how the security services (the police, judiciary and intelligence services) operate. It highlighted flaws in the Belgian security architecture, helping to explain why the terrorist networks behind the 2015 and 2016 attacks had not been dismantled in time.

717. The Joint Intelligence Centre (JIC) and Joint Decision Centre (JDC) were created to strengthen information sharing between the police, the judiciary and the intelligence services. Initially set up within the Brussels district, these structures were extended in 2023 to cover all five districts of Belgium. These centres, which focus on counter-terrorism, promote closer coordination and a rapid response to terrorist threats through regular discussions between the relevant stakeholders. The JICs bring together, at varying intervals depending on the jurisdiction, the main counter-terrorism stakeholders (intelligence services – VSSE, SGRS; the Coordination Unit for Threat Analysis (OCAM); police – DJSOC[212]/Terrorism and the Federal Judicial Police) as soon as new relevant information is identified. Regular consultations are also held at least once a month – and sometimes every week, as in Brussels – to ensure a continuous exchange of information between the intelligence services, the police and the public prosecutor's office, ensuring that information is shared in a systematic and coordinated manner. In addition to the JICs, JDCs have been set up to determine how to handle terrorism-related cases and TF cases more quickly. More specifically, they determine which authority is best placed to handle a case and take the most effective action. See the box below for details of how JDCs work.

[210] The French parliamentary committee report on the measures taken by France to combat terrorism since 7 January 2015. The committee visited Brussels and Molenbeek, a town often mentioned in connection with terrorist attacks, such as the attack on the Jewish Museum in Brussels (May 2014), the attack on the Brussels-Paris Thalys train (August 2015) and the attacks in Paris on 13 November 2015. https://www.assemblee-nationale.fr/14/rap-enq/r3922-t1.asp

[211] Committee tasked with investigating the circumstances surrounding the attacks at Brussels-National Airport and Maelbeek metro station. https://www.lachambre.be/FLWB/pdf/54/1752/54K1752008.pdf

[212] Belgian Central Directorate for Combating Serious and Organised Crime

Box 9.2. How Joint Decision Centres (JDCs) work

The JDCs provide a framework for continuous assessment of T/TF cases and joint decision-making between magistrates, investigators and intelligence services.

- The JDC's decision is largely based on the analysis prepared by the JIC, which is jointly developed and signed by all its partners.
- Files are classified according to their level of seriousness and risk with the aim of assessing their 'actionability', i.e. the need for and feasibility of taking action, taking into account the intentions and logistical and financial capabilities of the suspects.
- Decisions are based on specific criteria, such as the credibility, immediacy and scale of the threat.

One notable example is the large number of 'money collectors' files, where an investigation that started out as financial quickly turned into a terrorism-related case as a result of information sharing. This type of collaboration has helped prevent TF activities from going unnoticed.

718. This JIC/JDC process, launched in Brussels in 2018 and given a formal framework in a confidential circular[213] in October 2024, has brought new impetus to the detection of TF. Any new data potentially linked to terrorism is now included and analysed, even if no link has been confirmed. However, although more structured, this detection remains focused on a limited number of already identified targets, limiting visibility of potential emerging threats or networks operating outside conventional systems (e.g. informal transfers, virtual assets, donations in kind). This integrated approach improves understanding of financial flows linked to terrorist networks, but there is no statistical data to measure precisely the number of TF cases actually detected in this way. The effectiveness of this system also depends on the ability to continue active coordination efforts and anticipate new financing patterns, particularly through emerging technologies and informal financial networks.

719. Furthermore, the CTIF, despite holding most of the financial intelligence in Belgium (see IO.6), does not systematically participate in the JIC/JDC process where TF is involved. Its participation is on an ad hoc basis, when invited as an expert, which is also the case for the tax authorities. To date, no such invitation has been made. This means that, since their creation in 2018, these inter-institutional coordination platforms have not had direct and systematic access to CTIF information and data, such as STRs. This also limits their ability to quickly integrate financial intelligence into operational decision-making. The use of intermediary channels, in particular via the intelligence services or OCAM, can lead to delays, loss of contextual information and even blind spots in the assessment of a TF case by the JIC/JDC. This situation can hamper the detection of the financing aspect in structures focused primarily on counter-terrorism. There are no figures available to assess the extent to which these mechanisms are used in identifying and dealing with TF cases.

720. *Local Task Forces* (LTFs)[214] also play a role in gathering data from the field, with the aim of monitoring known targets and identifying cases that may be linked to TF at an early stage. They interact with the JIC/JDC platforms and help with referring cases initially classified as ordinary cases but which in fact show signs of TF to the Federal Prosecutor's Office. *Local Integrated Security Units* (LISU-Rs),[215] which work to prevent radicalisation and extremism, also interact with the LTFs. The local police representative

---

[213] CoI 16/2024 of 09/10/2024 on the JIC/JDC procedure.

[214] LTFs are set up at the level of each judicial district and bring together the police, justice and intelligence services, facilitating the exchange of operational information on individuals or networks suspected of radicalism.

[215] These units, which focus more on social prevention, are coordinated by the mayor and bring together a representative of the local police, social services and prevention services and, where necessary, other relevant partners (e.g. representatives from the education sector and local associations).

acts as a liaison between the LTFs and the LISU-Rs, ensuring that weak signals are passed on and taken into account in the judicial process via the JICs/JDCs.

721. Although these local platforms ensure effective coordination between the various counter-terrorism stakeholders and foster a multidisciplinary approach to detecting signs of radicalisation early, it is not clear whether they are adequately informed or aware of the challenges of CFT, or whether they receive adequate feedback from the police and judicial authorities on TF matters. In practice, there is no evidence that they have contributed to either instigating or supplementing TF investigations.

Infographic 9.1. Strategy on Extremism and Terrorism

Source: OCAM, Strategic Note on Extremism and Terrorism, September 2021 [link]

722. OCAM,[216] however, plays an important role in detecting and analysing terrorism/TF threats. In particular, it is involved in maintaining and updating the *Banque de données communes* (BDC),[217] which can be searched and shared by all stakeholders, including the CTIF. Support services are required to inform OCAM and provide it with information in the form of confidential notes or reports. In investigations, OCAM sometimes provides strategic notes, particularly on the use of innovative payment methods, such as virtual assets or decentralised platforms.

723. OCAM adopts a two-pronged approach to threat analysis:

a) Its micro analysis is particularly useful to JICs for the operational management of investigations. It provides investigators with information on threats to or from individuals or networks linked to TF. It is largely fed by the BDC, which is managed by OCAM. In this regard, OCAM is responsible in particular for ensuring information is

[216] CUTA is the federal centre of knowledge and expertise that assesses the terrorist and extremist threat in Belgium and to Belgian citizens and interests abroad. It also coordinates the response to it. The unit operates under the supervision of the Belgian Ministers of Justice and the Interior. CUTA carries out its tasks independently. This independence guarantees neutral and objective threat assessments.

[217] The Common Data Bank on Terrorism, Extremism and Radicalisation (BDC T.E.R.) is a dynamic database created in 2016 and managed by CUTA. It is a tool for sharing information in real time, fed by partner services, including the police and intelligence services.

shared between all counter-terrorism and TF services (including intelligence, internal security and the armed forces).

b) At the same time, its macro analysis is used to monitor major general trends in terrorism, confirm and support findings made in the field, and raise awareness among partner services of new trends, phenomena and/or threats.

724. Lastly, OCAM is required to provide ad hoc analyses on specific topics or certain files. For example, in an investigation into a suspicious financial scheme, it may cross-reference data with other sources and provide strategic insight into possible links with previously identified networks. This work helps to prioritise investigations and optimise investigators' resources.

725. Belgium does not have statistical data on the number of TF cases. However, the on-site visit confirmed that the JICs/JDCs have handled all investigations.

726. In addition, all cases handled by the terrorism section of the Federal Prosecutor's Office systematically involve a parallel financial asset investigation. Currently, around 10% of these cases focus primarily on TF offences. This percentage, which was significantly higher in the past, has fallen sharply following the defeat of the Islamic State terrorist organisation. This led to a temporary spike in TF cases, particularly those linked to Belgian FTFs travelling to Syria and the phenomenon known as Syrian Wallets (see Box 9.1).

9.2. Prosecuting and convicting different types of TF

9.2.1. TF prosecutions

727. In cases involving terrorism and its financing, the decision to open a criminal investigation is taken by consensus following a collective assessment of the cases by the JICs/JDCs. At the JDC stage, a collegial decision is taken with the local and federal public prosecutors and the coordinating director of the local police on how to proceed with the JIC's proposals. Based on the JIC's analysis, the authorities have several options: either to open a judicial file, to launch an intelligence investigation (carried out by the intelligence services) or to take action to prevent potential wrongdoing (possibly by way of an existing related judicial file). The JDC may decide to postpone its decision to allow the authorities to continue refining the information. In the very rare instances where no consensus is reached, each authority remains bound by its legal role. The Federal Prosecutor's Office could then, in theory, request that a judicial file be opened.

Table 9.2. Number of new terrorism cases opened by the Federal Prosecutor's Office

2019	2020	2021	2022	2023	2024
86	95	64	54	70	not disclosed

Source: Federal Prosecutor's Office

728. While this system is effective in detecting terrorist activities and prevents the opening of unfounded investigations, its effectiveness in combating TF depends on the agility of the process and the responsiveness of the authorities to emerging threats, in particular through the proactive detection of TF cases by using weak signals to good advantage. Financial analysis needs to be strengthened to address the emergence of new financing channels, such as virtual assets, opaque legal structures and certain NPOs.

729. In Belgium, there are no prosecutors specialising exclusively in TF, but each district prosecutor's office has at least one prosecutor responsible for terrorism cases. Jurisdiction is shared between districts

prosecutor's offices and the Federal Prosecutor's Office, but in practice the latter handles all cases related to terrorism or TF through its dedicated section, which comprises seven prosecutors specialising in terrorism, including two TF specialists.

730. The district prosecutor's office reports any case with a link to terrorism to the JICs/JDCs, and if a criminal case is opened, it is then assigned to the Federal Prosecutor's Office. Only cases in which minors are involved in terrorism or TF are exempt from this central control and are dealt with by the youth justice system and appropriate local authorities. This centralisation of TF prosecutions at the federal level ensures case handling is consistent and improves coordination with the investigative services. The lack of prosecutors specialising exclusively in TF within the Federal Prosecutor's Office is offset to some extent by the two TF specialist prosecutors. The Federal Prosecutor's Office also organises 'MONITOR' meetings to monitor on ongoing terrorism and TF cases (see box below).

731. The Belgian system is unique in that it has a strategic prosecutor (head of the terrorism section) within the Federal Prosecutor's Office who is responsible for the strategic coordination of prosecutions relating to terrorism and TF. Without managing operational investigations, the strategic prosecutor maintains an overall view by participating in the main steering bodies, such as the national terrorism expertise network (REN-Terro) and MONITOR meetings.

Box 9.3. MONITOR meetings

- Meetings are organised every six weeks by the Federal Prosecutor's Office, chaired by the strategic prosecutor responsible for the terrorism section. They are attended by all partners involved in combating T/TF, including specialist prosecutors, the police, the intelligence services, OCAM and the CTIF.
- These meetings provide an opportunity to review and discuss new judicial files, progress in major cases, information shared between partners and specific problems encountered. They foster smooth operational coordination and real-time information exchange and strengthen inter-agency cooperation, including at the international level, in particular with foreign prosecutors specialising in T/TF cases.
- The active participation of the CTIF and OCAM enables reports to be processed more quickly and in context. Their analytical contributions are supplemented by their direct knowledge of the individuals and contexts discussed at these meetings, thereby optimising the effectiveness of investigations.
- These meetings also provide an opportunity to address broader issues, new trends and problems encountered in both counter-terrorism and TF.

732. The Federal Prosecutor's Office has internal follow-up mechanisms, including a regularly updated dashboard[218] for cross-functional monitoring and a 'digital tagging' tool to aid in the identification of TF cases. Decisions and/or difficulties encountered are discussed at MONITOR meetings, and each decision on terrorism or TF is set out in a memo written by the principal prosecutor, which is distributed to the entire terrorism expertise network, including the specialist prosecutors in district prosecutor's offices. However, this is not a structured feedback mechanism specific to TF cases. The lack of such a mechanism limits to some extent the ability to capitalise on lessons learned from TF cases, which slows down process improvements, the early detection of TF and the sharing of best practices.

[218] Updated and sent to the strategic prosecutor every 1 to 2 months. This tool provides an overview of all cases and their progress, allowing prosecutors to identify those that may warrant faster processing or resource adjustments.

733. The investigation may come to a standstill, in particular when it stagnates or makes no progress without clear justification. In these situations, the case may be referred to the Pre-Trial Division, which will review the content of the investigation and identify any obstacles. However, this procedure is extremely rare: it has only been used twice in six years.

734. The caseload is difficult to quantify precisely, as prosecutors do not work on these cases on a daily basis. Many files that have been open for several years involve international cooperation, which slows down their processing (see IO.2). On average, each federal prosecutor handles approximately 40 cases simultaneously, across all areas. With regard specifically to TF, each prosecutor handles around two to three cases per year, with two prosecutors mainly involved in these cases, resulting in a maximum of 36 cases between 2019 and 2024. In practice, federal prosecutors have priority access to resources and generally obtain the support they request. However, this preferential allocation has an unbalanced effect: it exacerbates the chronic understaffing of district and general prosecutor's offices, which have not had the resources they need for several years. Furthermore, the lack of specialised resources within the police (DSJOC) is a major challenge, particularly given the changes in the way funds are transferred, such as virtual assets. This lack of capacity continues to be a structural problem (see IO.7).

9.2.2. TF Convictions

735. The judicial handling of TF cases in Belgium is structured around a specialised organisation, with divisions dedicated to terrorism and judges experienced in this field. A special terrorism division has been set up in Brussels to handle all cases related to terrorism and its financing for the Brussels judicial district. In some instances, these cases may be referred to the Court of Assizes. Other specialised divisions also exist in Liège, Charleroi, East Flanders and Antwerp, although the vast majority of T/TF litigation is concentrated in Brussels and Antwerp.

736. The allocation of TF cases may also take into account the nature of the offences. For example, TF cases involving hawala and other similar service providers may be referred to divisions specialising in economic and financial crime. This approach is justified by the complexity of financial schemes, which require specific expertise in unconventional financial flows. In 2024, four TF cases involving these types of flows were investigated, a figure that was consistent with previous years. As explained in the previous section, detecting these cases is particularly complex, as the transactions do not always pass through the traditional banking system. These cases are often uncovered by chance in the course of other legal proceedings, particularly through phone tapping or special investigation methods. These cases are difficult to quantify precisely and are often more complex to investigate. Nevertheless, a banking investigation is always carried out, even when the initial evidence is apparently limited.

737. However, TF cases involving individuals travelling to conflict zones are generally investigated by specialised terrorism divisions comprising three judges.[219] These cases, which are often small in scale, always include a banking and financial investigation to identify financing sources, assess logistical support networks and detect any links to terrorist organisations. This division of responsibilities ensures an approach that combines expertise in illicit financing and the analysis of terrorist dynamics, thereby optimising how TF cases are handled by the judiciary.

738. The vast majority of cases prosecuted for TF result in an actual conviction, with 46 of the 60 convictions between 2020 and 2024 for TF pursuant to Articles 140/141 of the Penal Code, or almost 60% of the total number of cases (see table below). Acquittals remain relatively rare, with only nine of the 79 cases over the same period being acquitted (i.e. one in 10 cases). This shows that the courts are keen to

[219] The terrorism division of the Brussels Criminal Court handles cases related to terrorism and TF in the Brussels judicial district. Other specialised divisions also exist in Liège, Charleroi, East Flanders and Antwerp, although the majority of cases are centralised in Brussels and Antwerp, where the prosecutor's offices generally handle these cases at the federal level.

prosecute and punish perpetrators for TF activities when there is sufficient evidence. Furthermore, alternative or additional charges (e.g. TF combined with an offence under the Payment Services (PSD2) Law or the AML Law) show that there is some flexibility in the judicial approach. This suggests that, even when terrorist intent cannot be fully established, courts resort to alternative grounds to ensure some form of punishment, particularly in cases involving informal transfer networks (see section 9.5). In some cases, the criminal justice response has been softened due to procedural circumstances (exceeding the reasonable time limit) or sentencing being deferred despite proven TF offences. This lenient measure was motivated by specific factors, including the cooperation of the defendant, the isolated nature of the offence and family circumstances raised in mitigation. Although governed by guidelines, this type of decision raises questions about the clarity and consistency of the criminal law framework in cases of 'small-scale TF' (see next section).

Table 9.3. Results of court rulings related to TF and PSD2/AML legislation (2019–2024)

Criminal justice response	Number of files (per defendant)		Criminal classification
Convictions	60	76%	46 for TF (140/141 PC) (i.e., around 60% of the total number of convictions) 7 for TF + PSD2/AML laws 7 for offences under Banking/AML laws
Acquittals	9	11.5%	9 (100%) for TF cases (140/141 PC)
Deferral of sentencing	9	11.5%	9 (100%) for TF cases (140/141 PC)
Other (referral to court of appeal, etc.)	1	1%	1 TF case (140/141 PC)
Total	79	100%	68 for TF (140/141 PC) 9 for TF + PSD2/AML laws 2 for offences under PSD2/AML laws

Source: Evaluation team (based on information provided by the Federal Prosecutor's Office)

739. With regard to the length of TF proceedings, Belgium adopts a balanced approach between risk prevention and respect for the rights of suspects. Thus, conditional release for six months during the investigation of a case appears to be a pragmatic measure, aimed at avoiding excessive pre-trial detention and allowing for behavioural assessment before considering more severe sanctions or probationary measures. However, this approach has to contend with the sometimes protracted nature of TF investigations, which can last up to two years, making it more difficult to monitor suspects and adapt legal measures. Monitoring mechanisms can be put in place to limit potential risks, particularly if suspects remain at liberty throughout this period. Probation officers monitor suspects after their release, at the request of the prosecutor's office. In complex cases, such as the Hawala case, there have been periods of pre-trial detention lasting two years. Although long, this period is not considered excessive in sensitive cases involving opaque financial flows and international criminal networks.

9.3. Effectiveness, proportionality and dissuasiveness of sanctions

740. In cases combining T and TF, the sanction is a single blanket sentence, making it difficult to distinguish between the specific sanction for TF and that related to terrorism. This approach is pragmatic but may raise issues in terms of assessing the proportionality of sanctions in relation to the specific seriousness of the financial offence. The prevention of terrorism appears to be a priority when applying sanctions, which may mean that the TF aspect is integrated into a broader response rather than being

punished individually. The primary goal is therefore to neutralise the overall threat rather than to distinguish between offences on strictly financial grounds.

741. The main sentence (imprisonment) almost always includes a probationary period for part of the prison term. In practical terms, the accused serves part of their sentence in prison (usually half), while the remainder is suspended subject to certain conditions. During the probationary period, they must comply with certain obligations defined by the judge, such as a ban on reoffending, judicial supervision or financial restrictions. If these conditions are not met, the suspended part of the sentence may be reinstated and enforced. Additional measures may be imposed, such as limiting banking access to a single account in Belgium, thereby preventing suspicious transactions abroad and reducing the likelihood of reoffending.

742. Where recovering the funds is possible, they are confiscated to prevent them from being used to finance other criminal or terrorist networks (see IO.8). The fines imposed remain proportionate. *See the T Spasorti case below.*

Box 9.4. T SPASORTI case

IO.9 relevance: This case highlights the challenges of investigating TF, especially when clandestine payment methods such as hawala are used. Despite late detection and technological obstacles, the investigation successfully dismantled a structured and clandestine network involved not only in money laundering but also in terrorist financing, in this case for Islamic State.

Facts: This case highlighted the use of a hawala network to finance the escape of female members of Islamic State detained in camps in northern Syria, enabling them to rejoin the terrorist organisation. This case was not detected by the CTIF, but was indirectly uncovered as part of an investigation into the financing of the escape of these female members of Islamic State, which also resulted in a conviction.

The investigation, which lasted nearly four years, involved significant resources, including financial analysis, phone tapping and a year of active surveillance. The arrest of the suspects marked a turning point, revealing a large amount of evidence, including messages confirming the financial transactions. However, the lack of appropriate IT tools posed a challenge in analysing the data due to the volume of data recovered from the seized devices and the need for translation.

Conviction: The case followed the JIC/JDC procedure, resulting in the opening of a judicial file in 2020. The final judgement was handed down in November 2024 – six defendants were prosecuted for operating a hawala system in the form of payment services, constituting an offence under banking law. All six defendants were convicted:

The court upheld all charges against them. These included violation of banking law, ML offence (Art. 505(1) of the Penal Code), participation in a criminal organisation, terrorist financing (Art. 140/141 of the Penal Code), tax evasion and social security and tax fraud.

The judge established that some of the defendants were not just low-level operatives ('small fry'), but key players in the system. They were found to be co-perpetrators of TF and ML offences due to their active role in organising and facilitating transactions without authorisation or supervision. The ruling is based on a form of objective liability, demonstrating knowledge of and conscious involvement in the illegal system.

Confiscation and sanctions: The court upheld the confiscation of approximately €973,000 (out of the €4 million requested by the Public Prosecutor's Office).

	Main prison sentence (with partial probation)	Fine	Subsidiary (alternative) sentence *for non-payment*	Confiscation
Defendant 1	*8 years without parole*	€80,000	3 months' subsidiary imprisonment	€472,184.83
Defendant 2	5 years, *including 3 years without parole* and 2 years suspended for 5 years	€40,000	3 months' subsidiary imprisonment	€472,184.83
Defendant 3	4 years, *including 2 years without parole* and 2 years suspended for 5 years	€8,000	2 months' subsidiary imprisonment, suspended for 3 years for half of the subsidiary sentence [220]	€19,674.37
Defendant 4	3 years, *including 18 months without parole* and 18 months suspended for 5 years	€4,000	2 months' subsidiary imprisonment, suspended for 3 years for half of the subsidiary sentence	€9,837.18
Defendant 5	3 years	€8,000	2 months' subsidiary imprisonment	/
Defendant 6	200 hours (failing which, 20 months' subsidiary imprisonment)	€1,600	2 months' subsidiary imprisonment	/

743. The imposition of prison sentences and confiscation orders combined with probation measures ensures that convicted offenders are monitored on a long-term basis. However, its effectiveness depends on the proper monitoring of probation conditions and on the ability of the authorities to identify and confiscate misappropriated funds, which often requires international cooperation.

744. This type of sentence combines a tough stance with an incentive for rehabilitation. A prison sentence ensures immediate punishment and acts as a deterrent. In practice, imprisonment may occur either during the investigation (through pre-trial detention ordered by the investigating judge) or when the judgement becomes final. Furthermore, although statistical data on reoffending in relation to TF is limited, no cases of reoffending have been recorded in Belgium to date. Probation provides offenders with a chance of reintegration, while maintaining judicial pressure on them. A fine is a financial penalty, with an alternative prison sentence if they do not pay, thereby reinforcing the coercive nature of the sentence.

745. The enforcement of the sentence is the responsibility of the Public Prosecutor's Office, in particular with regard to the confiscation of assets derived from TF. Confiscation is a major challenge, as it often requires international cooperation. In practice, confiscation measures are only effective to a limited degree, as in many cases (with the *T Sparsori* case being somewhat of an exception), the funds have already been transferred abroad, particularly to jurisdictions that are not especially cooperative (see IO.2).

746. However, the judge may sometimes impose a *simple suspension of sentencing* - a measure in which the judge acknowledges the defendant's guilt, but postpones the pronouncement of the sentence. This is neither an acquittal nor a formal conviction. In this case, no conviction appears on the criminal record, provided that the defendant do not reoffend within a specified period. This suspension may also be subject to specific conditions, in which case it is referred to as a *probationary suspension of sentencing*. If these conditions are not met, the judge may revoke the suspension and impose a sentence. This measure is rarely handed down for TF offences (nine times between 2020 and 2024, or 11.5% of cases – see table in section 9.2). In a very specific and isolated instance, the judge deferred sentencing in a case where there were clear TF indicators, including proven facts, large amounts transferred over a long period, the use of

[220] If the fine is not paid, the defendant faces two months in prison as an alternative. However, half of this additional sentence (one month) is suspended for three years. If the defendant does not pay the fine, they will serve one month in prison immediately. The other month of imprisonment will be suspended, provided that they comply with certain obligations for three years (e.g. no reoffending, compliance with the rules imposed).

clandestine channels and aggravating circumstances (explicit intention to support the rise through the ranks of an active member of Islamic State). See the *Loute case* in the box below. The decision to impose a simple suspension of sentencing in this case, without conviction or effective sanction, may be perceived as conveying a weak signal regarding the combat the TF. Such a decision seems at odds with the sustained efforts made by the police and judicial authorities between 2017 and 2023. It does not constitute a response that has sufficient dissuasive effect in terms of CFT and could potentially undermine the credibility of the entire judicial system in this area.

Box 9.5. Loute (V.L.) case

Background: Between 2013 and 2015, V.L. transferred a total of €63,039 to her son, a member of Islamic State (IS) linked to the Paris attacks, through money collectors, bank loans (consumer credit), the sale of shares she had inherited and the sale of her house. The case was opened in 2017, triggered by a referral from the Paris National Anti-Terrorism Prosecutor's Office.

The investigation, supported by searches, phone tapping and a letter of request to Turkey, revealed that V.L. was aware of the legal risks and was deliberately financing her son to help him rise through the IS's ranks. Conversations with another mother and information from the CTIF confirmed that her motives were not humanitarian.

Outcome: On 18 January 2023, the Brussels Court of Appeal found V.L. guilty of TF, but granted a simple suspension of sentencing for three years. The decision took into account mitigating circumstances (family ties, no previous convictions, involvement in community work), despite aggravating factors that were not punished (explicit desire to support her son within the IS hierarchy that went beyond humanitarian purposes, conscious knowledge of the legal risks and the impact of the funds sent).

747. While Belgium refuses to accept any form of plea bargaining in TF cases, it does have a case management tool available called *judicial probation (probation prétorienne)*, which is an alternative to prosecution. Unlike a plea bargain, this is not based on an agreement between the accused and the prosecutor's office, but on a unilateral decision by the prosecutor not to refer the case to the investigating judge. It is akin to a dismissal of the case subject to conditions. However, in practice, the suspect's consent is essential, given the probationary period involved in this mechanism. The suspect is summoned, cautioned, informed of legal obligations, and placed on probation. It therefore acts more as a warning signal than a real criminal sanction.

748. Between 2018 and 2024, judicial probation was used on eight occasions in TF cases, making it a relatively uncommon measure (see box below for some examples). The decision to grant conditional suspensions is based on a range of mitigating factors, including active cooperation or confessions by suspects to investigators, family circumstances where the funds are intended for relatives, small amounts, an isolated offence without a structured pattern, and, lastly, the desire to avoid disproportionate consequences associated with a criminal conviction. The humanitarian argument appears to be key in these cases, particularly to avoid a strictly punitive response when criminal intent is ambiguous.

Table 9.4. TF cases closed by judicial probation (TF type and amounts) (2018–2024)

Date	TF type and amounts	Motives
October 2018	Money sent to a family member (niece) in the region (in 2016) Amounts: €2,902 (1 month between the 2 transfers)	– Acknowledgement of the offence and active cooperation – Specific family circumstances (sending to niece and her children) – One-time, non-recurring offence – Negative impact of a conviction for TF
Sept. 2020	(Detected as part of the Syrian Wallet project) Money sent to a family member (son) in the region (2016–2017) Amounts: €2,140 (over 5 month in 3 transfers)	– Small amounts – Acknowledgement of the offence/cooperation – Specific family circumstances – Negative impact of a conviction for TF
March 2021	Funds sent to the region Amounts: €1,900 (in 4 transfers)	– Humanitarian motivation, no ideological intention to support terrorism
May 2021	Money sent to a family member (brother) in the region in 2017 Amounts: €1,642 (in several transfers over one month)	– Small amount – No 'terrorist' ideology – Specific family and personal circumstances – Collaboration
June 2024	Money sent to a family member (brother) in the region in 2015 Amounts: €1,570 (single transfer)	– Small amount – No 'terrorist' ideology – Specific family and personal circumstances – Collaboration

Source: Federal Prosecutor's Office

749. However, taking small amounts into account as a mitigating factor is more debatable. In the case of terrorist financing (TF), even modest sums can have a significant operational impact, particularly when the beneficiary is affiliated with a terrorist group. While judicial probation is a useful mechanism in certain emotionally sensitive situations, it must not be applied to TF in such a way as to inadvertently create a loophole that could be exploited by malicious actors. Strict controls must therefore be maintained on the use of this procedure. In practice, in the eight cases where this measure was used, the judicial authorities did not identify any repeat offences. However, its effectiveness – like that of the suspension of the sentence – depends on rigorous monitoring.

750. However, it is worth noting that automatic referral to court if an ideological element is detected, regardless of the amount involved, contributes to the dissuasive effect, provided that this element is clearly identifiable, which is not always the case. Furthermore, as long as the case is not time-barred, it can be reopened at any time. This provides an additional guarantee in that probation does not mean permanent impunity and prosecution can be reactivated in the event of new suspicious behaviour, subject once again to active monitoring and the ability to detect any repeat offences.

751. In some cases, closing a case with judicial probation provides an opportunity to carry out surveillance, identify networks, map suspicious financial flows and observe changes in the suspect's behaviour before considering more decisive action, if necessary. However, this practice appears to contradict the stated, albeit informal, principle of 'zero tolerance', which seems to be the repressive message advocated by the authorities in relation to TF.

9.4. National counter-terrorism strategies and activities

752. Belgium does not currently have a national strategy specifically focused on TF. Combating TF is part of the broader operational framework for combating terrorism (TER Strategy), which guides actions in the areas of prevention, detection and prosecution (see IO.1).

753. In terms of criminal policy, the Public Prosecutor's Office nevertheless advocates a 'zero tolerance' approach to TF, even though this position is not formalised in a strategic document. While this approach is mainly aimed at excluding discretionary decisions not to prosecute, it does not exclude alternatives to prosecution, such as praetorian probation, which is discussed in more detail in the previous section.

754. The CTIF plays a unique role in Belgium's CFT system, taking a similar approach to that used for ML. It produces analytical reports that can be shared with intelligence services or, if needed, with prosecutor's offices. Although it is not a permanent member of the Intelligence and Security Coordination Committee (CCRS), which assists the National Security Committee responsible for strategic coordination of the national response to terrorism and TF (see IO.1), the CTIF has presented the TF NRA to the CCRS, thereby contributing to strategic thinking. The CTIF also chairs the TF platform, which brings together the intelligence services, the police, OCAM and other stakeholders to assess risks and coordinate TF-related actions. Although the CTIF also helps to coordinate CFT-related actions, political and strategic decisions are taken within the CCRS.

755. The sharing and use of information is a central pillar of Belgium's response to terrorism. A structured ecosystem around OCAM, which acts as a fusion centre, ensures that information from the police, the intelligence services, prosecutor's offices, the CTIF and other stakeholders is centralised, cross-checked and used in a coordinated way. This structure not only provides an up-to-date picture of the T and TF threat, but also ensures rapid and concerted action, in particular through TF platforms, local task forces and JIC/JDC meetings (see section 9.1). Consequently, the lack of a strategic document specific to TF does not appear to have any impact on the implementation of TF objectives and activities at operational level.

756. Although cooperation channels exist at all levels – strategic, operational and judicial – the effectiveness of the system depends above all on the quality, speed and contextualisation of the information provided. Efforts are still needed to improve the accuracy of analyses, particularly given the current academic nature of national TF risk analysis (see IO.1), and to take better account of certain weak signals, particularly those of a financial or informal nature. A more proactive approach, made possible in particular by increasing the number of investigators and augmenting their expertise in emerging areas such as informal channels and virtual assets, would further strengthen the operational T/TF framework.

757. The involvement of the private sector, in particular certain financial institutions and digital platforms with advanced monitoring, behavioural analysis and anomaly detection capabilities useful for the early detection of TF, is still limited in Belgium. The lack of structured public-private partnerships is currently slowing down efforts to adapt Belgium's response to emerging terrorism- and TF-related threats.

9.5. Alternative measures used where TF conviction is not possible (e.g. disruption)

758. In some TF cases, such as those where hawala is used as a payment system, Belgian courts sometimes adopt a cumulative approach to offences (see table in section 9.2). In these cases, the judge generally charges the defendant with multiple offences, demonstrating that hawala is not limited to a simple breach of the requirements applicable to authorising financial institutions, but is often a vehicle for wider criminal activity. The offences charged include:

a) Offence under the Payment Services (PSD2) Law[221] on payment institutions (Art. 149, 1º): Hawala operates as an unregulated payment service, in direct violation of the PSD2 and AML/CFT laws.
b) ML offence (Art. 505 para. 1 PC): This type of system is often used to integrate money of illegal origin into the mainstream economy.
c) Criminal organisation (Art. 324bis PC): When a structure is set up to facilitate clandestine financial flows, it is classified as an organised criminal structure, which carries heavier sanctions.
d) Tax and social security fraud: Due to the clandestine nature of hawala, the income generated by these activities is not declared, leading to prosecutions for tax fraud and often also for social security fraud, particularly in relation to undeclared workers or undeclared self-employment.

759. The judge may not uphold the charge of TF (Art. 140 and 141 of the Penal Code) in TF cases where neither terrorist intent nor the final destination of the funds can be clearly proven. If the investigation fails to establish that the money actually financed terrorist activities, then the TF classification becomes legally fragile. In these cases, the judge will instead consider reclassifying the offence under the PSD2 or AML laws, where offences are easier to establish based on the available evidence and a conviction is more likely. The judge may also consider that the money transferred came from an illegal or undeclared source, without needing to establish an explicit link to terrorism. This approach makes it possible to punish those involved in clandestine financial systems, even when there is insufficient evidence of a direct link to terrorism.

760. Other non-criminal measures may also be used as alternatives, such as freezing assets in the country (see IO.10) or procedures for withdrawing or invalidating identity documents, such as passports. The law also allows for the administrative dissolution of non-profit organisations (NPOs) when they are involved in TF or activities contributing to radicalisation. However, these cases are still very rare. The competent authorities have identified very few cases of NPOs being directly involved in TF. There are therefore very few cases where this measure has been used. In the few cases identified, the NPO's involvement and the financial sector's preventive blocking of banking transactions generally result in these entities quickly becoming dormant entities.

[221] Law of 11 March 2018 on the status and supervision of payment institutions and electronic money institutions, imposing prudential obligations on them in terms of governance, internal control and compliance. Article 149 1° imposes criminal sanctions for carrying out payment institution or electronic money institution activities without the required authorisation.

10 Terrorist financing preventive measures and financial sanctions

The relevant Immediate Outcome considered and assessed in this chapter is IO.10. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 6 and 8 and elements of R.14, 15, 16, 26, 30, 31, 32, 35, 37, 38 and 40.[222]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

Targeted financial sanctions (TFS) for TF

a) Belgium has an inter-institutional framework for identifying targets to be designated under United Nations Security Council Resolutions 1267/1989, 1988 and subsequent resolutions. In practice, Belgium does not play an active role in proposing designations for inclusion on UN sanctions lists.

b) Belgium applies without delay TF related TFS adopted under UNSC Resolutions (UNSCRs) 1267/1989, 1988 and 1373, and under the EU and national sanctions regimes.

c) Belgium focuses on implementing TF related TFS adopted at national level. Proposals for designations to the national list are subordinated to the existence of a police or a judicial investigation, which limits the scope of targets for freezing measures and is contrary to FATF requirements (R 6). Belgium has never asked a third country to give effect to freezing measures taken at the Belgian level. No national designations have been made in response to a request from a third country.

d) Only certain financial institutions (FIs) have taken freezing measures in relation to designated persons and entities, but the amount of assets frozen is consistent with the country's TF risk profile. Nonetheless, no virtual assets have ever been frozen, even though virtual assets are one of the TF modi operandi identified by Belgium.

e) FIs demonstrate varying levels of understanding of their obligations on TF related TFS. The very low level of understanding among DNFBPs and the fact that no assets have been frozen by these entities or by customs authorities triggers questions over the effectiveness of TF related TFS in Belgium.

[222] Recommendations 1, 2, 6, 7, 8, 14, 15, 16, 32, 38 and 40 are under review; see Technical Compliance Annex.

f) The SPF Finance-Treasury, which is responsible for monitoring compliance with the freezing obligations relating to TFS, has not identified any serious failure to comply with the freezing obligations to date.

g) Supervision of compliance by FIs with their TFS obligations is partially satisfactory. At least one case of non-implementation of TF related TFS was identified by the supervisors but did not result in sanctions. The authorities supervising DNFBPs, with the exception of the SPF Economy, have a limited understanding of TFS mechanisms and do not adequately ensure that the DNFBPs comply with their obligations over TF related TFS.

Non-Profit Organisations (NPOs)

h) Authorities have a broad understanding of the NPO sector exposed to TF risk. To date, 2,493 NPOs are recognised as meeting the FATF definition. These are essentially NPOs that have applied for tax approval in order to reduce taxes. Of these, 93 receive public funding for development cooperation projects, particularly in conflict zones. However, no precise data is available on NPOs active in at-risk areas without state subsidies, which limits the complete identification of NPOs with significant TF risks. This situation reflects a partially reactive identification, based mainly on reports of suspicious transactions to the CTIF and tax approval procedures.

i) Belgium conducted a risk assessment specific to NPOs based on an inter-institutional approach, which identified several categories of NPOs considered to be more exposed to TF risks. However, this assessment does not provide a quantified mapping by type of NPOs, area of operation or financing method, which makes it impossible to precisely quantify the number of NPOs at risk and to measure the levels of vulnerability specific to each organisational profile. As a result, the effective identification of NPOs at TF risk relies mainly on intelligence services and information from counter-terrorism efforts, rather than on a strategy based on objective criteria and dynamic mapping of the sector.

j) The monitoring of the non-profit sector is fragmented across several competent authorities (SPF Justice, CTIF, OCAMOCAM, VSSE, federal police), without a dedicated central unit or inter-institutional coordination structure. This fragmentation of responsibilities limits the overall vision, the circulation of information and responsiveness.

k) NPOs identified as being more exposed to TF risk are not subject to mitigation measures specifically targeted at this TF risk, but are subject to some general controls (fiscal or related to accreditation for the granting and use of public funds). Although these controls have a mitigating effect, they do not constitute measures specifically designed to address the risk of TF. In addition, this approach does not take into account NPOs operating in at-risk areas that have not applied for tax approval or received public funding. Furthermore, for small and medium-sized at-risk NPOs, the administrative burden associated with these obligations appears disproportionate.

l) In general, awareness-raising activities with NPOs have recently been initiated by SPF Finance, in particular through a series of large-scale webinars. More targeted and in-depth awareness-raising on the specific TF risks to which the sector is exposed, as well as more practical support, have not been implemented at this stage.

Key Recommended Actions (KRAs)

Belgium should:

a) Remove the requirement of the existence of a police or judicial information or investigation from the designation criteria, so that persons and entities can be targeted more actively (in line with the technical compliance shortcomings identified in R.6 – see TC Annex).

b) Strengthen inter-institutional coordination between competent authorities, for example by considering the designation of a contact point responsible for coordinating and monitoring the NPO sector within the CFT framework, in order to ensure a coherent overview, facilitate the sharing of relevant information and allow for a more structured, targeted and proportionate monitoring of the TF risks identified.

c) Define and implement proportionate and targeted monitoring and mitigation measures for NPOs identified as being at high TF risk, taking into account the structural and operational features of the non-profit sector (in line with the technical compliance shortcomings identified in R.8 – see TC Annex).

Other Recommended Actions

Belgium should:

Targeted financial sanctions

a) Proactively propose designations to the UN for TF related TFS under the sanctions regimes relating to UNSCRs 1267/1989 and 1988.

b) Fully implement the freezing measures taken at the Belgian level under UNSCR 1373 by requesting that third countries implement them more consistently where relevant.

c) Strengthen awareness-raising measures on TFS and their importance in combating the financing of terrorism, and develop guidelines based on examples and typologies for customs authorities to identify assets and property belonging to persons subject to TFS, for DNFBPs to fully understand their obligations, and for DNFBP supervisory authorities to establish effective supervision.

d) Conduct DNFBP inspections on the effective application of obligations linked to TF related TFS to identify any non-compliance, and sanction such non-compliance more actively.

e) Conduct more thorough verification of the effective application of TF related TFS during FI inspections to prevent that potential breaches are not detected.

NPOs

f) Develop a proactive approach to identifying NPOs at risk of TF by developing an approach based on objective criteria and better use of existing data (such as the UBO register, dissolutions) to supplement the current declaration mechanisms.

g) Develop a classification of NPOs based on their level of exposure to TF risk, using objective criteria, in order to adapt monitoring requirements to the risk profiles, and thus reduce disproportionate burdens on legitimate, low-risk small organisations.

h) Strengthen awareness-raising efforts by making them more targeted, practical and adapted to the specific risk profiles of NPOs, particularly those operating internationally (especially in at-risk areas), including through the distribution of practical tools, case studies and feedback on TF risks.

i) Strengthen efforts to trace the end use of funds destined for at-risk areas, in collaboration with the non-profit sector, with a view to developing a framework for documenting and verifying the use of funds in the field, based on practices already in place in the sector.

j) Implement a formal consultation framework with the non-profit sector, such as a memorandum of understanding, to structure information sharing and ensure regular monitoring of compliance issues, particularly in the context of humanitarian or international actions are.

Overall Conclusions on IO.10

With regard to TF related targeted financial sanctions, Belgium has amended its legal framework to allow for the immediate application of UN designations. Since 2016, it has mainly used designations on the national list based on proposals from OCAM to target assets linked to TF. However, the criteria for designation on the national list and for proposing designations to the 1267/1989 and 1988 Committees are conditioned to the existence of criminal proceedings, which limits the wider use of TFS as a preventive tool to deprive terrorists, terrorist organisations and individuals who finance terrorism of the resources and means to finance or support terrorist activities and organisations. Belgium mainly takes a reactive approach to TF related TFS and does not play an active role in proposing designations for inclusion on the UN and EU TF sanctions lists. In addition, Belgium has never asked a third country to give effect to freezing measures taken at the Belgian level.

The amount of funds frozen as a result of UN, EU and national designations is low overall, which is consistent with the TF risks to which Belgium is exposed. However, the type of assets frozen is not fully aligned with the TF modi operandi identified in Belgium. These mainly involve the use of cash and virtual assets. No notifications of freezing measures in respect of TF related TFS have been received from DNFBPs or the customs authorities. However, the very low level of understanding among DNFBPs of TFS mechanisms and the associated obligations has an impact on the full effectiveness of TF related TFS measures in Belgium.

With regard to NPOs, the effectiveness of the system is undermined by limitations in the identification of NPOs exposed to TF risk, in particular the lack of a comprehensive and regularly updated mapping of NPOs at risk of TF. Existing controls – tax auditing, financial reporting, or oversight related to public subsidies – are not tailored to TF risks, and tend to overlook non-subsidised NPOs or those operating in high-risk areas without registration. Furthermore, for some NPOs, existing requirements are onerous but ineffective in detecting potential TF abuse. As a result, the overall effectiveness of the framework is weakened by an incomplete and inconsistent approach that is still insufficiently based on targeted TF risk assessments.

Major improvements are required.

Belgium is rated as having a Moderate level of effectiveness for IO.10.

Immediate outcome 10

761. The evaluation team has based its conclusions on the information and documentation provided by Belgium, on discussions with the competent authorities, supervisory authorities and the private sector.

10.1. Implementation of TF-related targeted financial sanctions without delay

10.1.1. Implementation without delay

762. Since 2019, Belgium has had a legal framework enabling the immediate implementation of targeted financial sanctions (TFS) for TF, pursuant to United Nations Security Council Resolutions (UNSCRs) 1267/1989 and 1988. Designations made under this framework have been immediately applicable in Belgium since 2019 (Law of 2 May 2019, Art. 236, see TC Annex, R 6), which compensates for delays in transposing UN designations at EU level. Belgium implements designations adopted at European level through Regulations which are immediately applicable in Belgium from the date of their publication in the Official Journal of the EU (Regulation (EU) 2001/2580 and Regulation (EU) 2016/1686, see TC Annex, R 6).

763. Belgium has also been implementing TF related targeted financial sanctions adopted at the national level since 2016. The use of national designation and asset freezing measures became a more important tool in combating TF since the attacks in Paris and Brussels in 2015 and 2016. Although this national TF freezing mechanism has been planned since 2006,[223] it was only implemented in May 2016, when Belgium first added names to the list.[224] The Belgian list is updated within 24 hours of a new designation being published in the Belgian official journal (*Moniteur belge*) by means of a Royal Decree (RD) identifying the person to be added.

10.1.2. Proposals for designations to the UN Sanctions Committees and the EU

764. Belgium rather takes a reactive approach and does not play an active role in proposing designations for inclusion on the UN and EU TF sanctions lists. As of 14 February 2025 (end of the on-site visit), Belgium had co-sponsored eight designation proposals at the request of other countries under UNSCRs 1267/1989 and 1988. Belgium has not submitted any proposals to the UN Sanctions Committees to designate Belgian nationals. At the EU level, Belgium submitted one designation proposal and supported eight co-sponsorships initiated at the request of other countries (Germany, France and the Netherlands) involving seven individuals and three entities.

765. Since 2015, Belgium has set-up an inter-institutional framework for identifying targets to be designated under UNSCRs 1267/1989, 1988 and subsequent resolutions. The Minister for Foreign Affairs is the competent authority for designating individuals at the national level and subsequently submitting proposals to the UN Sanctions Committees and to the Working Party on Restrictive Measures to Combat Terrorism (COMET) at the EU level. The Minister coordinates with the National Security Council (NSC) (responsible for strategic coordination of the national response to terrorism and TF, see IO.1) after consulting the various national intelligence services (for details, see TC Annex, R 6). The authorities meet monthly to discuss designation proposals.

766. The Belgian judicial authorities are also consulted and must give their approval to the proposed designation to not compromise ongoing criminal proceedings.[225] However, the Belgian authorities indicate that they have no examples of a proposal that has been opposed by the judicial authorities. The CTIF is not one of the authorities formally consulted, but it does indirectly provide financial information for the database of the Coordination Unit for Threat Analysis (OCAM) and allows the authorities involved in the designation process to access financial information about the potential target.

[223] Royal Decree of 28 December 2006

[224] See RD of 30 May 2016 and the list of other Royal Decrees issued to add or remove persons from the Belgian national list.

[225] In the case of sponsorship by Belgium, the prosecutor's office is simply consulted.

767. The procedure and criteria for TF-related designations are set out in two confidential NSC decisions of 11 December 2018 (UN designations)[226] and 20 November 2023 (EU designations),[227] which the evaluation team was able to review. These decisions set out relatively broad criteria for deciding whether to propose a name for a UN or EU designation. They include the existence of a threat to Belgian interests, which must be demonstrated to justify a designation proposal. However, Belgium also makes the designation proposal conditional on the existence of criminal proceedings in Belgium against the person or entity concerned, which limits Belgium's effectiveness in proposing new designations to the Sanctions Committees (see TC Annex, R 6).

10.1.3. Designations on the national list under UNSCR 1373

768. Belgium makes more frequent use of designations under its national TF sanctions list when the targets are not already covered by sanctions established at the EU level. OCAM initiates the formal designation process. The judicial authorities must also give their approval, and a number of services are consulted (see TC Annex, R 6). Proposals are sent to the NSC for approval, with final approval resting with the Council of Ministers. Each amendment to the national list must be set out in a Royal Decree and the revised national list is published in the Belgian Official Journal ('*Moniteur belge*'). The procedure for delisting is the same, as is the procedure for proposing the designation of persons on a third country's national list or for a third country to request additions to the Belgian list. The national list is reviewed at least twice a year[228] and when information reaches the competent authorities about possible intentions of potential targets to leave or return to Belgium or finance terrorism.

769. The level of requirement for inclusion on the Belgian national list goes beyond the existence of 'reasonable grounds' or a 'reasonable basis'. Only behaviour constituting criminal offences can lead to a designation. Proposals for designation are conditional on the existence of a criminal proceeding, which limits the scope of potential targets for freezing measures (see R 6, c.6.2 (d)). The College of Prosecutors General states that the Federal Prosecutor's Office preserves judicial proceedings and does not agree to a designation measure on the national list before the target is subject to pre-trial detention or conditional release, charged or brought before a court. As of 14 February 2025 (end of the on-site visit), the Belgian national sanctions list included 265 individuals, including 257 former foreign terrorist fighters who had left Belgium and were in a jihadist conflict zone, and eight former terrorist fighters who were en route to Belgium or had returned to Belgium after travelling to a jihadist conflict zone. OCAM was responsible for initiating all designations on the national list. No entities (non-profit organisations, foundations, etc.) appear on the national list. The Belgian authorities have made a deliberate choice to designate only natural persons, due to the ease with which legal persons can be created, dismantled and restructured and the indirect ability to freeze funds that natural persons may hold through control or significant participation in a legal person.

770. The composition of the sanctions list is largely consistent with the country's risk profile (see the Introduction), although non-profit organisations (ASBLs) are identified as at risk in the TF NRA and TF cases have involved ASBLs (see IO.9).

771. However, Belgium does not fully implement national designations under UNSCR 1373. Since 2016, Belgium has not requested any third country to implement freezing measures taken at the Belgian level, confirming Belgium's lack of a proactive approach to TF related TFS. No national designations have been made in response to requests from third countries. Belgium has received five informal requests from third

[226] National Security Council Decision – Procedure for determining the Belgian position within the UN Security Council with regard to the targeted application of sanctions against individuals, legal entities and others.

[227] National Security Council Decision – Effective and uniform procedure for determining the Belgian position within the EU Council with regard to the application of restrictive measures against individuals, legal persons and other entities as part of efforts to combat terrorism.

[228] CUTA reassesses the designations every six months to determine whether the persons listed still have an intention to cause harm.

countries (France in 2017 and 2020, Saudi Arabia in 2017, Turkey in 2018 and the United States in 2018). However, no link could be established with Belgium and these requests were therefore unsuccessful as no formal request was made.

772. Belgium periodically reviews the listing or delisting of national designations. Since 2016, the authorities have delisted at least 45 individuals on the national list. However, one of them was subsequently relisted. OCAM initiated all but one of the requests. These delistings followed an update of the threat assessment by OCAM and its partners, which concluded that these designated persons no longer met the criteria for designation, in accordance with the circular of 7 September 2015. The SPF Finance granted exemptions to the freezing measures, in accordance with the procedures laid down for this purpose, including for the repayment of existing debts to the State and for the payment of legal costs and various essential expenses should the person concerned be imprisoned, which are valid grounds for exemption.

10.1.4. Notification of designations

773. Belgium considers that reporting entities are themselves responsible for monitoring changes to the sanctions lists applicable in Belgium. New designations on the national list of national financial sanctions under UNSCR 1373 are published in the Belgian Official Journal ("*Moniteur belge*") and are listed on the SPF Finance website,[229] in its capacity as the authority responsible for implementing freezing measures (see the Introduction). The SPF Finance also maintains a consolidated list on its website, which includes all financial sanctions in force under the various sanction regimes adopted by the UN and the EU, as well as those included on the Belgian national list. When a UN designation is made just before a weekend or public holiday, the list is not updated immediately. There is therefore a risk of delay in implementing freezing measures following a UN designation if entities have not obtained the information by other means. However, the fact that the freezing obligation under UNSCRs 1267/1989, 1988 and subsequent resolutions is immediately applicable in Belgium and that financial institutions (FIs) use other tools to keep themselves informed of new designations mitigates the impact of these delays to a certain extent. Since 2024, the system for updating the consolidated list and notifying subscribers to this list has been automated. This notification system allows anyone interested to receive immediate updates on changes to the list. The SPF Finance also notifies the supervisory authorities of any changes by email. However, the Belgian authorities have not indicated how long it took to update the system before 2024.

774. The vast majority of FIs use various automated tools developed by private companies to assist in screening existing and potential customers against sanctions lists. Some FIs maintain their own internal lists (see IO.3). There have been cases where reporting entities did not use the most up-to-date lists. Reporting entities must ensure that the lists they use are complete and accurate, and this must be checked periodically by all supervisors. The National Bank of Belgium, as the supervisory authority, checks the completeness and accuracy of the lists used by its reporting entities during its inspections.

775. DNFBPs mainly perform manual checks using public sources, including the SPF Finance list. Some DNFBPs do not carry out the necessary checks against official lists, which they confuse with high-risk country lists (see IO.4).

10.2. Identification and deprivation of terrorist funds or other assets

776. The funds and other assets of designated persons are only identified and frozen to a certain extent by some FIs (banks and insurance companies). Notifications of frozen funds and economic resources to the SPF Finance are the main source for identifying the assets of listed persons. Reporting entities (and all other

[229] UN and EU designations are also published in the Official Journal of the EU and are consolidated in the list maintained by the European Commission (EC), which is accessible through a similar notification system when updates are made.

persons concerned) are required to notify SPF Finance of any freezing measures taken in relation to TFS for TF. If the person's name is the same (false positives), the SPF Finance initiates an identification procedure with the security services, the police and OCAM to confirm whether the transaction falls within the scope of TFS. If it does not, the transaction is then unfrozen.

777. In practice, only FIs notify the SPF Finance when the designated persons have an account or have entered into a financial contract with them. The SPF Finance has not yet received any notifications from DNFBPs or the customs authorities in connection with TF related TFS. The SPF Finance may receive notifications from other government departments, such as the SPF Finance's General Administration of Heritage Documentation, which provides information on real estate owned (jointly) by individuals included on the sanctions list. The number of notifications issued by these departments has not been provided, with the exception of one notification from the National Pensions Office, which froze the pension of a person on the national sanctions list.

778. The financial information held by the CTIF (see IO.6) and the information gathered in the course of terrorism investigations and prosecutions, where these have a financial component (see IO.9), are also important sources of information for identifying and depriving terrorists, terrorist organisations and individuals financing terrorism of funds and other assets.

779. The SPF Finance carries out verification measures for each person on the national sanctions list, to determine whether they hold funds and other assets in Belgium. These verification measures have not led to identifying any breaches. They are mainly carried out by checking with the central register for financial accounts and contracts (PCC, see IO.5), which establishes whether the individuals listed have a bank account or have entered into a financial contract with one of the Belgian FIs. The SPF Finance also searches the many databases in Belgium, such as the register of beneficial ownership (UBO), to check whether the people on the list are the beneficial owners of a legal entity (see IO.5). In practice, these checks have not identified any individuals or entities that should be subject to freezing measures. The checks carried out by the SPF Finance should in theory also enable it to identify FIs that have not notified it that they maintain a bank account or have entered into a financial contract with a listed person. In practice, the checks have not identified any such failures.

780. Between 2019 and 2024, Belgium froze EUR 8 548 under the EU Al-Qaida regulations and EUR 84 000 relating to individuals included on the national list. These freezing measures were in response to notifications from banks and insurance companies. One immovable property was also subject to a freezing measure. These relatively low amounts are consistent with the country's TF risk profile (mainly micro-financing of terrorist cells, lone actors and former foreign terrorist fighters; see IO.1 and IO.9). However, the type of assets frozen (mainly bank account balances) is not consistent with the terrorist financing methods identified by Belgium, which places greater emphasis on the use of cash and virtual assets (see IO.1 and IO.9). The fact that no assets have been frozen by customs authorities or DNFBPs and the limited understanding of these entities raises concerns that transactions falling within the scope of TF related TFS may not have been identified, raising questions about the full effectiveness of TFS measures in Belgium. Nevertheless, Belgium has carried out some seizures and confiscations in TF cases (see IO.8 and IO.9).

781. Since November 2024, SPF Economy's Basic Banking Service division, which is responsible for designating the credit institution (CI) that must provide basic banking services to entities subject to de-risking measures, has been checking national and international TFS for TF lists when reviewing applications from legal entities requesting this service. Because no such checks were carried out before November 2024, the Basic Banking Service Division could refer entities potentially subject to national TFS imposed by foreign authorities to CIs (see IO.1 and IO.3).

10.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

782. In 2019, the reform of the legal framework applicable to non-profit organisations (NPOs) harmonised the obligations of NPOs with those of companies, strengthening their financial transparency and governance (see the Introduction). However, the assessment of Belgium's compliance with R 8 reveals persistent challenges in identifying and managing TF risks related to NPOs (see TC Annex).

10.3.1. Identification of at-risk NPOs

783. The Belgian non-profit sector comprises approximately 135,828 NPOs (February 2025).[230] These organisations cover a wide range of fields, including social, cultural, educational and health-related activities. Some are active internationally, particularly in humanitarian aid and development cooperation. There are 2,493 NPOs that fall within the FATF definition (see R 8). These are mainly NPOs that have applied for tax approval for tax reduction purposes. Among these, 93 receive government subsidies for development cooperation projects, particularly in conflict areas. Belgium does not have accurate data on NPOs operating in at-risk areas without public funding.

784. These 2,493 NPOs appear to cover the vast majority of Belgian entities falling within the FATF definition. However, some organisations at risk of TF (despite falling within the FATF definition) may voluntarily waive approval to avoid transparency requirements and official supervision. This weakens the effectiveness of the current system, which relies on a voluntary approach motivated by tax advantages rather than a structured and proactive mechanism for detecting TF risks among NPOs (see R 8).

785. Belgium conducted a risk assessment specific to NPOs in 2019, updated in 2024, based on an inter-institutional approach.[231] This assessment identified several categories of NPOs considered to be most at risk of TF:

- 93 NPOs active abroad, particularly in humanitarian aid and conflict zones, are particularly vulnerable, as the aid they provide could be diverted for terrorist or TF purposes. These are NPOs receiving public funding.
- Religious NPOs (local religious communities or non-profit associations under the Belgian Companies and Associations Code, see IO.5) may pose a significant risk of TF when they support or promote extremist ideologies or serve as a direct or indirect channel of funding for radical networks.[232] There is no census of the number of religious NPOs in Belgium, but at the end of 2024, there were 3,866 recognised local religious communities (places of worship).
- Inactive or dormant NPOs that can be reactivated to transfer funds without going through regulated banking systems.
- NPOs excluded from the regulated financial system due to abusive de-risking practices, which may lead them to resort to unregulated money transfer channels, such as hawala. They are mainly detected by the intelligence services and through judicial and police investigations. In 2023, 46 NPOs applied for basic banking services; in 2024, 36 did so. These channels are not generally monitored by the banking sector, limiting the ability to detect TF risks at an early stage.

786. The 2019 risk assessment is based primarily on the analysis of suspicious financial transactions reported to the CTIF, as well as on cross-referencing data between intelligence, police and judicial services.

---

[230] This sector includes non-profit associations (NPAs), international non-profit associations (INPAs), public utility foundations (PUFs) and private foundations (PFs).

[231] Involving, in particular, SPF Justice, the CTIF, the Coordination Unit for Threat Analysis (OCAM), intelligence services (VSSE and SGRS) and the federal police.

[232] This also includes the 1,876 entities audited as part of the BELFI project.

It also takes account of trends observed in other at-risk sectors and information from development cooperation for NPOs operating abroad. It also provides a clear understanding of the main TF risk factors, such as international operations (particularly those carried out in conflict zones), sources of funding and jurisdictional risks. The assessment also highlights the risks associated with NPOs active in conflict zones and the risks associated with NPOs involved in hawala or other informal money transfer systems. The authorities pay particular attention to these financial flows.

787. Despite the efforts made to assess risk factors, significant limitations remain in identifying NPOs at risk of TF. These assessments do not provide a quantitative mapping by type of NPO, area of operation or funding method, which makes it impossible to quantify precisely the number of at-risk NPOs and to measure the vulnerability levels specific to each organisational profile (see c.8.1b). This lack of granular analysis reduces the authorities' ability to target prevention measures in a proportionate and effective way. The current assessment is based mainly on STRs submitted to the CTIF and tax approval procedures. However, this approach is report-based and reactive, and fails to take advantage of several opportunities to proactively identify at-risk NPOs. Several identifying sources, such as data from the UBO register and on dissolutions of dormant NPOs, are available, but they are not used to their full potential. The authorities make up for this with information from the intelligence and police services obtained in connection with efforts to combat terrorism, extremism and radicalisation. However, these sources do not systematically cover all NPOs operating in Belgium and abroad. At the judicial level, legal proceedings have been brought against certain NPOs for TF offences, confirming that there are actual cases in the sector.

788. As a result, some NPOs at high risk of TF may potentially slip through the monitoring net, especially those that have not applied for tax approval and those operating in areas that do not receive public funding.

10.3.2. Monitoring mechanisms

789. Belgium has introduced financial and administrative monitoring mechanisms for NPOs. These include enhanced supervision for subsidised NPOs, including mandatory audits for large organisations and the administrative deregistration of 'dormant' (inactive) NPOs.

790. For example, NPOs that want to operate internationally and be eligible for Belgian public funding must get official accreditation,[233] valid for ten years. This accreditation process is rigorous and demanding: it involves an external assessment conducted by a private company appointed by the DGD, which examines risk management, personnel management, financial transparency and several cross-cutting issues (integrity, gender, governance, etc.). Furthermore, to issue tax certificates entitling them to tax relief, NPOs must obtain approval from SPF Finance. However, although these tax procedures are well regulated, they are unable to detect NPOs that deliberately choose to evade any form of monitoring. These NPOs may, however, be subject to targeted checks by the police and intelligence services.

791. Enhanced supervision for subsidised NPOs is applied uniformly, without differentiation based on TF risk level (as Belgium does not classify NPOs based on their exposure to TF). As a result, even NPOs with links to high-risk jurisdictions or operating in conflict zones are not systematically subject to enhanced supervision.

792. Monitoring measures are in place for religious NPOs that support or promote extremist ideologies, or serve as a direct or indirect channel of funding for radical networks identified as at risk in national assessments (see previous subsection). These measures include checks carried out by the intelligence

[233] Accreditation issued by the Directorate-General for Development Cooperation and Humanitarian Aid (DGD) of SPF Foreign Affairs, Foreign Trade and Development Cooperation.

services and the police on individuals managing NPOs linked to recognised local religious communities,[234] although there are no figures available to measure the extent of this. Checks are also carried out on ministers of religion and delegates of non-denominational philosophical organisations paid by SPF Justice. Indirectly, NPOs linked to this sector are also subject to the obligations laid down by the Companies and Associations Code and the UBO register.

793. Although not strictly speaking a monitoring measure, the BELFI project (see box below) is an interesting initiative that can be used to monitor this category of at-risk NPOs. Initially focused on NPOs linked to radicalism, its scope has since been broadened. It has led to the closure of 277 organisations. While this project had the potential to identify organisations that could be at risk of TF, the results obtained are not directly linked to the detection or prevention of TF. The most frequently observed offences relate to illegal residence, social security fraud, drugs, weapons and false documents. This mechanism is therefore not a targeted or continuous monitoring mechanism specifically focused on NPOs at high risk of TF.

Box 10.1. BELFI project

Context: launched in 2014, this pluri-dimensional project arose from the observation that nearly 90% of Belgian foreign terrorist fighters were receiving public funding.

Objectives: One of the objectives of the 'police' component of this plan is to combat the illegal economy. BELFI aims in particular to detect and control fraud associated with security risks, targeting both natural and legal persons. It focuses in particular on NPOs (NPAs) suspected of providing logistical, financial or organisational support for radicalisation or terrorism.

BELFI is not an investigation unit but a detection and monitoring structure. When a case requires further investigation, it is referred to the competent investigation services. The monitoring results are systematically entered into police databases.

Outcome: A total of 1,876 entities were audited, resulting in the closure of 277 structures, 20 arrests and 482 detentions of illegal immigrants. The most common offences were illegal residence, social security fraud, drugs, weapons and forged documents.

794. For dormant NPOs, Belgium has also strengthened its monitoring mechanisms for the sector since 2024 by launching a campaign to deregister and dissolve inactive NPOs, with a view to cleaning up the UBO register and preventing abuse, particularly from a CFT perspective:

a) Automatic administrative deregistration, provided for by the law of December 2023, targets entities that do not comply with certain fundamental obligations, such as failure to register in the UBO register and/or to update their articles of association in the Belgian Official Journal for more than seven years. If the NPO fails to regularise its situation after receiving a formal notice, it will be automatically deregistered, with the possibility of reinstatement if it returns to compliance. On this basis, 35,897 NPOs had been deregistered as of 14 February 2025.

b) Judicial dissolutions, carried out since 2019 by certain commercial courts, target dormant NPOs based on objective criteria (e.g. failure to file accounts, have directors or publish statutory documents). A total of 13,186 NPOs have been dissolved since the launch of this initiative, including 2,422 between 2023 and 2024.

795. While these measures have reduced the number of dormant entities that could be reactivated to transfer funds for TF purposes, deregistrations and dissolutions are triggered by formal administrative

[234] That is, local religious communities or non-profit associations falling within the remit of the Companies and Associations Code, as part of the procedure for recognising local religious communities, pursuant to the circular of 21 October 2024.

criteria (non-publication of accounts, failure to update UBOs, etc.) and do not result from an assessment based on specific TF risks. This is neither a risk-based approach, nor does it involve proportionate targeting based on NPOs' actual TF risk exposure. It may leave active but at-risk NPOs off the radar if they are administratively compliant. Furthermore, without a support mechanism, active NPOs that are not well structured or simply do not comply with certain reporting requirements could be wrongly removed from the list.

796. For the last category of NPOs identified as being at risk of TF, the BNB's supervision of the de-risking practices of financial institutions helps to identify and prevent abusive exclusion practices (see IO.3). However, it is difficult to fully assess the scope of this supervision without figures or concrete evidence.

797. However, overall, monitoring measures – such as enhanced transparency requirements, financial flow justification requirements or high compliance expectations imposed by financial institutions as part of AML/CFT – are applied fairly consistently across the entire non-profit sector, without any differentiation based on actual exposure to TF. This generic approach, which is not based on the actual risk of TF, has several consequences:

- It imposes the same accounting, administrative and governance obligations on all NPOs, including those whose activities have no connection with sensitive areas or channels.
- It creates a disproportionate burden, particularly for small humanitarian or social organisations seeking public funding, which struggle to meet requirements designed for much more exposed entities. Some NPOs have reported the practical difficulties that this regulatory burden places on their day-to-day operations.
- It may dilute the resources available to authorities, preventing them from focusing their efforts on NPOs that are genuinely at risk of TF.
- It undermines access to financial services for some legitimate NPOs. There have been reports of account freezing and delays in subsidy payments. They may also be denied the right to open an account if no individual risk assessment is carried out. This cautious but blanket approach may encourage financial institutions to engage in de-risking practices, preferring to exclude certain NPOs rather than manage a risk they perceive as complex. Between 2023 and 2024, 82 NPOs applied for basic banking services, accounting for 15.3% of the total 536 applications – a significant proportion that indicates their partial exclusion from the banking system. Although the BNB has not observed any widespread de-risking in the sector, tangible effects are evident on the ground. Some association federations have also entered into dialogue with Febelfin to prevent unjustified exclusion. This type of measure, which is more about mitigation than monitoring, can help prevent certain NPOs from being marginalised.

798. Furthermore, monitoring of the is fragmented across several authorities (SPF Justice, CTIF, OCAM, VSSE, federal police), with no central body dedicated to supervising TF risk in NPOs, which limits coordination and responsiveness.

10.3.3. Measures to mitigate the risk of terrorist financing

799. At the same time, Belgium has introduced several measures aimed at reducing the risks of TF in the non-profit sector. In general, NPOs must comply with strict financial transparency requirements, including the obligation to register beneficial owners in the UBO register, file annual accounts and, for some, undergo mandatory external audits, particularly those receiving public funding or operating internationally. Large NPOs must also comply with IATI standards (see R 8), ensuring full traceability of funds to their final destination, which is good practice in TF risk management. However, these measures are mainly geared towards protecting the integrity of the non-profit sector, rather than specifically designed to target NPOs at risk of TF, thus reducing their effectiveness in detecting possible suspicious activities.

800. Numerous measures have also been taken for the religious sector identified as at risk in national risk assessments, although not all of these are monitoring measures. The 3,866 religious communities recognised in Belgium, which are public institutions, may be linked to non-profit associations subject to the Companies and Associations Code and to accounting and UBO obligations. They are also subject to checks by the police and intelligence services (statistical data not provided).

801. Belgium also relies on several inter-institutional cooperation mechanisms to support the exchange of information between authorities involved in combating TF, including the judicial authorities, the CTIF, OCAM, the State Security Service, the SGRS and the federal police. These exchanges facilitate the cross-referencing of information from STRs, judicial investigations and intelligence. The information is also integrated into the *Banque de données communes* (BDC) (see IO.9), thereby centralising data collected on NPOs reported as potentially at risk of TF. Lastly, this cooperation involves occasional meetings between the authorities and representatives of the non-profit sector, aimed at raising awareness of the risks and strengthening supervision without hindering the legitimate activities of NPOs. However, these mechanisms are limited due to the absence of a central entity dedicated to monitoring at-risk NPOs and the lack of a standard framework for coordinating the monitoring and implementation of mitigation measures.

802. Some mitigation measures are implemented by the sector itself. For example, NPOs working in international development cooperation tend to have internal mechanisms for monitoring funds, although the extent of these mechanisms varies depending on the organisation. Some have developed structured internal control systems, including tools for evaluating their local partners, particularly with regard to the use of funds. Supervising the use of funds in the field often relies on the involvement of local teams. These processes ensure that funds can be traced to their destination to a certain extent. NPOs receiving public funding are also subject to structured monitoring by SPF Foreign Affairs, covering annual reports, strategic dialogues, field missions and mandatory audits carried out by an auditor, regardless of their size. However, this monitoring remains largely internal or dependent on the donor, with no harmonised mechanism at the national level. Furthermore, as it ultimately relies on local partners and organisations, full and effective traceability of the final use of funds cannot be completely guaranteed. This limitation, which is not unique to Belgium, reflects a structural difficulty in ensuring full supervision of the use of funds in operational settings.

10.3.4. Awareness-raising and capacity building for NPOs

803. Belgium has launched a number of awareness-raising initiatives aimed at NPOs, in collaboration with federations in the sector. In 2024, training courses and webinars were organised by SPF Economy, SPF Justice and SPF Finance, focusing on UBO obligations, financial sanctions, TF risks and applicable regulations. A one-to-one written campaign was also sent to NPOs falling within the FATF definition. The sector itself plays an active role in promoting good governance, including among small organisations.

804. Some NPOs have also implemented internal measures, such as mandatory training on TF risks or the appointment of internal control officers. These steps are often motivated by donor requirements and reflect a commitment to professionalisation. At the same time, an 'Impact' coalition has been created to give structure to the dialogue between the voluntary sector and the authorities, making it easier for the sector to accept certain obligations that are seen as restrictive (particularly UBO).

805. Despite these efforts, the dissemination of information has been patchy. Small organisations and NPOs with limited connections to umbrella networks often receive less exposure to awareness-raising initiatives. The content of these initiatives is also considered to be too general and not sufficiently aligned with the sector's specific risk profiles, particularly for NPOs operating in conflict zones or receiving funds that are difficult to trace. The sector is pressing for more practical awareness-raising, using real-life examples and case studies.

806. Discussions take place between the authorities and the sector, in particular with SPF Finance, SPF Economy and SPF Justice, but these remain sporadic and informal, with the exception of the Dialogue Council.[235] The implementation of a more structured framework for consultation, such as a memorandum of understanding, would lead to more regular and systematic meetings, allow more formal feedback from the authorities and ensure better collective monitoring of compliance issues, particularly where humanitarian or international efforts are concerned.

10.4. FIs and DNFBPs understanding of and compliance with obligations

807. All natural and legal persons in Belgium are required to freeze the funds of persons or entities included on the UN, EU and national lists (Art. 8, §1, 3° of the AML Law and as described above).

10.4.1. Financial institutions

808. Financial institutions (FIs) demonstrate varying levels of understanding. Banks generally have a good understanding of their TFS obligations. The results of a horizontal review conducted by the BNB, reported in December 2024, show that credit institutions comply with their screening obligations for domestic and international transactions, although some shortcomings were found in domestic transactions. Some FIs do not necessarily carry out periodic and/or continuous re-screening of their customer databases.

809. The currency exchange offices and lenders visited during the on-site visit demonstrated a lower level of knowledge. The shortcomings relate in particular to the procedures and frequency of checks against the TFS lists. For example, one major lender indicated that it screens the lists once a month, but not at the start of a business relationship. The FSMA often has to remind institutions that TFS obligations are not risk-based but must be applied consistently to all customers.

10.4.2. DNFBPs

810. With the exception of a few legal professionals (notaries in particular), DNFBPs demonstrate a very low level of understanding of their TFS obligations. This is a vulnerability for implementing TF related TFS effectively and without delay. In general, DNFBPs of all sizes and across all sectors seem to be unfamiliar with the actual purpose of TFS, screening procedures, the frequency of checks and the authorities who must be notified of freezing measures. Some DNFBPs confuse the lists of high-risk countries with the lists of persons and entities subject to TFS. Even among DNFBPs that consult the SPF Finance-Treasury sanctions lists, there are significant shortcomings in understanding the mechanisms and objectives of TFS, which is particularly worrying. However, little support and very few tools are made available to DNFBPs, whose role in applying TFS is no less important.

10.5. Competent authorities monitoring and ensuring compliance with TF targeted financial sanctions

811. The SPF Finance-Treasury, which is responsible for implementing asset freezing measures, also monitors compliance with the obligations of reporting entities.[236] It receives asset-freezing declarations, and reporting entities are required to report to it whether or not they hold funds on behalf of the persons

[235] The Dialogue Council is a body for official discussions between SPF Justice, the Prime Minister, the Minister of Justice and representative bodies of recognised religions and non-denominational philosophical organisations.

[236] Art. 7 of the law of 13 May 2003.

and entities targeted by each new designation.[237] The SPF Finance then carries out its own checks, for example by regularly monitoring the Belgian bank accounts register. Failure to comply with targeted financial measures is punishable by an administrative fine of between EUR 25 and EUR 250 000. The SPF Finance may also pass the information on to the Prosecutor's Office, in which case offenders are liable to a criminal sanction of imprisonment for between eight days and five years and/or a fine of between EUR 250 and EUR 25 000.[238] To date, the SPF Finance has not identified any serious breach of the freezing obligations and has therefore not imposed any administrative sanctions or referred any cases to the Prosecutor's Office. Only one warning was issued to an FI in 2018 for failing to carry out checks on the freezing measures targeting two persons on the national list.

812. The AML/CFT supervisory authorities for FIs and DNFBPs are responsible for ensuring that reporting entities have developed and implemented effective internal control procedures and measures to comply with TFS obligations. Generally, compliance with targeted financial sanctions obligations is monitored alongside AML/CFT obligations.

813. The FI supervisory authorities carried out supervisory and awareness-raising activities among their reporting entities to ensure that FIs had put in place the necessary frameworks for implementing TF related TFS. These activities were relatively effective, particularly with regard to credit institutions. The BNB also carried out remote horizontal reviews based on questionnaires sent to credit institutions regarding their compliance with their TFS obligations in 2022 and 2024.[239] The BNB notes that credit institutions generally comply with their obligations for international transactions and observed an improvement between 2022 and 2024 in the screening measures adopted for domestic transactions, which the BNB now considers to be generally adequate and satisfactory. These reviews resulted in the BNB identifying a serious breach by one FI in its screening of sanctions lists following an inspection in December 2022. The Auditor is currently investigating this case. In December 2024, the BNB issued a communication to FIs reminding them of their internal control requirements. These various supervisory activities led the BNB to refine the granularity of questions relating to TFS obligations in the periodic questionnaires sent to FIs.

814. The FSMA uses periodic questionnaires and inspections to verify whether FIs are fulfilling their TF related TFS obligations. The FSMA has stated that it often has to remind FIs that TFS obligations are not risk-based and that checks must be carried out on an ongoing basis. In January 2025, it published the findings of a currency exchange offices inspection campaign, in which it identified room for improvement for the sector as a whole with regard to implementing TFS.

815. The DNFBP supervisory authorities have a limited understanding of TFS obligations, with the exception of SPF Economy, which has a very good understanding and, as part of its supervisory role over some DNFBPs, carries out the screening of several sanctions lists. During their inspections, the DNFBP supervisory authorities often check that a checklist exits on which the reporting entities must indicate that they have carried out a check of the UN, EU and national lists, or that screening procedures in place. However, they do not check whether these requirements are actually met or whether the reporting entities understand them.

816. Supervisory authorities offer little guidance and undertake few awareness-raising initiatives, with the exception of the accounting supervisory authority (ITAA), which proactively distributes changes to sanctions lists as soon as it receives them from SPF Finance and offers awareness-raising opportunities to its members, such as training courses and printed materials. Detailed TFS guidance for diamond traders were developed in 2021, but these appear to be rarely used and out of date.

[237] The duty to notify SPF Finance of freezing measures is limited by the professional secrecy to which lawyers are subject.

[238] Art. 4 of the law of 11 May 1995.

[239] Communication BNB_2024_19 / Results of the horizontal supervisory review of credit institutions' compliance with their obligations relating to targeted financial sanctions and domestic transactions | BNB.be

11 Proliferation financing financial sanctions

The relevant Immediate Outcome considered and assessed in this chapter is IO.11. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 7 and elements of R.1, 2 and 15.[240]

Key Findings, Recommended Actions and Conclusion and Rating

Key Findings

a) Belgium has carried out an initial national risk assessment (NRA) of proliferation financing (PF) that goes beyond the risks associated with potential breach, non-implementation or evasion of TFS obligations. This approach has provided a global understanding of PF risks and takes into account Belgium's specific context in this area, in particular the importance of the port of Antwerp. However, the identification, assessment and understanding the risks of breach, non-implementation and evasion of PF sanctions is not sufficient to ensure that the measures in place are sufficient to mitigate these risks. The private sector did not directly contribute to this analysis.

b) Belgium is not affected by any known geographic or demographic factors with the Democratic People's Republic of Korea (DPRK) that might facilitate proliferation and its financing or create increased vulnerability.

c) The National Security Council (NSC) is responsible for developing policies on combating the proliferation of weapons of mass destruction (WMD) and its financing. Belgium's 2021 National Security Strategy includes sections on combating proliferation but does not address the issue of financing. Belgium does not have a targeted strategy on PF, and the implementation of TFS is currently the only measure in place in Belgium specifically targeting PF. Operational cooperation between authorities that may hold information on PF has not yet contributed to identifying sophisticated schemes to evade PF related TFS.

d) Belgium has a legislative framework based mainly on European regulations to implement UNSCR 1718 and subsequent resolutions. The mechanism applicable to TF related TFS for TF(see IO.10). Belgium has not yet submitted any proposals for listing or delisting designations on the EU and UN sanctions lists relating to PF.

e) The SPF Finance-Treasury, the authority responsible for implementing PF related TFS, was first notified in 2024 of asset freezes by banks involving three transactions that may be indirectly linked to the DPRK. These freezing measures, although recent and limited, appear to be consistent with Belgium's PF risk level. However, reporting entities' understanding of TFS for PF is limited to identifying potential cases of breach and non-implementation of TFS, rather than identifying more sophisticated ways of evading PF related TFS.

[240] Recommendations 1, 2, 6, 7, 8, 14, 15, 16, 32, 38 and 40 are under review; see Technical Compliance Annex.

f) The supervision carried out on FIs is fairly satisfactory. However, the level of understanding and supervision of DNFBPs in relation to TFS for PF is low, which could affect their ability to identify and freeze PF-related property and assets.

Key Recommended Actions (KRAs)

Belgium should:

a) Deepen the national PF risk analysis on the basis of a contextual analysis of the different methods, trends and complex typologies related to non-compliance with, non-application of or the evasion of TFS for PF, and involve the private sector.

b) Develop and apply risk indicators to enable FIs, DNFBPs and customs and supervisory authorities to identify complex patterns of evasion of TFS for PF.

c) Conduct inspections of FIs and DNFBPs in relation to TFS for PF, targeting not only the mechanisms in place but also the effective detection of any failures to comply with freezing obligations, and provide for appropriate sanctions for any failures identified.

Other Recommended Actions

Belgium should:

a) Strengthen operational cooperation between the SPF Finance-Treasury and authorities holding information on proliferation-related risks and technological developments, to ensure that their understanding of the risks is kept up to date.

Overall Conclusions on IO.11

The framework applicable to PF related targeted financial sanctions is based primarily on European regulations and relies on an institutional structure that is similar to the one in place for TF. Belgium does not have a targeted strategy on PF, and the implementation of TFS is currently the only measure in place in Belgium specifically targeting PF. The freezing measures implemented, although recent and limited, appear to be consistent with Belgium's PF risk level. Belgium has conducted an initial national risk assessment that takes a comprehensive approach to PF risks. Nevertheless, the identification assessment and understanding of the risks of breach, non-implementation or evasion of PF sanctions is not sufficiently addressed to ensure that existing measures adequately mitigate these risks.

Furthermore, reporting entities' understanding of PF related TFS is limited to identifying potential cases of breaches and failure to implement TFS. The very low level of understanding among DNFBPs of their obligations over PF related TFS and the absence of financial or non-financial assets and property frozen by DNFBPs and customs authorities for PF related TFS raises concerns that transactions falling within the scope of PF related TFS may not be identified. This casts doubt on the full effectiveness of PF related TFS in Belgium. In light of this, Belgium has not fully demonstrated its ability to ensure that no funds or assets are made available, directly or indirectly, to entities and persons subject to TFS for PF. Major improvements are still required.

Belgium is rated as having a Moderate level of effectiveness for IO.11.

Immediate Outcome 11[241]

817. The assessment team has based its conclusions on an examination of the system in place in Belgium for applying targeted financial sanctions for proliferation financing (PF related TFS), the figures available on frozen assets,[242] and discussions with the Belgian authorities and the private sector.

818. At the end of the on-site visit (14 February 2025), relevant UNSCRs in force relating to PF were Resolution 1718 pertaining to the Democratic People's Republic of Korea (DPRK) and subsequent Resolutions 1874, 2087, 2094, 2270, 2321 and 2356. These Resolutions are transposed into Belgian law by European Regulation (EC) 2017/1509 and are directly applicable in Belgium.

11.1. Competent authorities co-operation and co-ordination to combat PF financing

11.1.1. Co-operation and co-ordination to develop and implement policy

819. The National Security Council (NSC) (see the Introduction and IO.1) is responsible for coordinating efforts to combat the proliferation of weapons of mass destruction (WMD) and its financing. The Coordination Committee (Intelligence and Security), which is responsible for coordinating and implementing the NSC's decisions, meets approximately once a month. It brings together all stakeholders involved in efforts to combat PF. The intelligence services (VSSE, SGRS), OCAM, the Federal Judicial Police and the SPF Foreign Affairs are permanent members of the Coordination Committee (Intelligence and Security). The SPF Finance-Treasury, which is responsible for implementing asset freezing measures, may also be represented on the Coordination Committee when the topics discussed relate to its remit.

820. Belgium's 2021 National Security Strategy includes sections on combating proliferation but does not address the issue of its financing. Similarly, PF is not addressed in the February 2025 government agreement, although combating proliferation is mentioned. Belgium does not have a targeted strategy on PF, and the NSC has not carried out any specific work in this area. The implementation of TFS is currently the only measure in place in Belgium specifically targeting PF.

11.1.2. Co-operation and, where appropriate, co-ordination for operational purposes

821. Frameworks for operational cooperation with authorities holding information on PF (i.e. the intelligence services (VSSE), Federal Prosecutor's Office, SPF Economy, SPF Finance (Treasury and Customs), as well as regional export control services) are in place. The cooperation frameworks established under the auspices of the SPF Foreign Affairs (see IO.10) ensure that consultation takes place on proposals for designations at UN and European level. The VSSE holds and shares information on proliferation with a view to preventing financial transactions originating in or passing through Belgium related to materials and technologies that could be used to produce or develop unconventional or highly advanced weapons systems, and to implementing national, European and international sanctions on proliferation, including TFS. The Advisory Commission for the Non-Proliferation of Nuclear Weapons (CANPAN), which is responsible for granting export licences and supervising exports of nuclear materials, equipment and technology, also holds and shares relevant information. Over the past five years, no applications for exports

[241] The TFS relating to the Islamic Republic of Iran set out in UNSCR 2231 ceased to apply on 18 October 2023 and are therefore not assessed in this report. The TFS provisions of UNSCR 1737 and successor resolutions have subsequently been re-applied (on 27 September 2025), but they are not covered in this assessment as this occurred after the end of the on-site period in January – February 2025.

[242] There are legal and regulatory requirements for keeping these statistics in Belgium, but they have not been implemented (see TC Annex, R 33).

to the DPRK have been submitted to CANPAN. In practice, the information available to these authorities has not to date identified any potential evasion of PF related TFS.

11.2. Understanding and mitigating the risks of breach, non-implementation or evasion of PF-related targeted financial sanctions

822. Belgium has no legal basis for requiring PF risks to be identified and assessed, nor a designated competent authority (see TC Annex, R 1). Nevertheless, it conducted an initial PF national risk assessment (PF NRA) in April 2024, coordinated by the SPF Finance-Treasury. The scope of the NRA has provided a global understanding of PF risks and takes into account Belgium's specific context in this area. However, the private sector was not directly involved.

823. The PF NRA concludes that Belgium's exposure to PF risk is low. It notes that Belgium is not affected by any geographic or demographic factors that might facilitate proliferation and its financing or create increased vulnerability. There are no proven economic ties between Belgium and the DPRK, and the North Korean diaspora in Belgium is small, consisting of only a few political refugees. The NRA considered certain vulnerabilities that could lead to a risk of PF and concluded that this risk is low, given the mitigation measures in place. The NRA covers the existence of Belgian companies active in the nuclear field and producing 'dual-use' (civilian and military) goods that could be diverted to WMD development programmes, the fact that Belgium is home to the port of Antwerp and financial institutions connected to the international financial system, and the diamond trade and the use of virtual assets. However, the NRA does not establish a clear link between these factors and the risk of breach, non-implementation or evasion of PF related TFS to which Belgium may be exposed.

824. With regard to the risk of breach, non-implementation or evasion of PF related TFS, the NRA identifies a risk of indirect financing made possible by the use of intermediaries, shell companies and legal arrangements to conceal the beneficial owner of funds and obscure illicit financial flows relating to PF. However, it lacks a more in-depth contextual analysis of the different methods, trends and complex typologies related to evading PF related TFS.

825. Lastly, some of the ML threats identified as having a potential impact in terms of evading PF related TFS are not addressed, including the existence of transnational organised crime groups and networks operating in Belgium and the development of networks with international connections involving countries potentially at risk of PF.

826. Belgium has implemented measures to mitigate PF risks, through the implementation of PF related TFS and their monitoring by the SPF Finance, and these are consistent with its risk assessment. On this basis, Belgium has not defined higher-risk and lower-risk scenarios.

827. FIs, particularly banks, generally have a good understanding of their obligations on PF related TFS. This is also of the case for FI supervisors, although the supervision carried out does not necessarily identify weaknesses in reporting entities' internal control procedures (see section 11.6). However, the level of understanding and supervision of DNFBPs on PF related TFS is weak, with the exception of SPF Economy (see section 11.5). This potentially impacts the ability of DNBFPs to identify designated persons or entities and more complex patterns of breach, non-implementation or evasion of PF related TFS. Identifying potential evasion of PF related TFS is also made more difficult by certain shortcomings in identifying beneficial owners (see IO.5).

11.3. Implementation of PF-related targeted financial sanctions without delay

828. Belgium primarily relies on European legislation to implement obligations relating to PF related TFS.[243] The mechanisms that apply to implementing TF related TFS established at the UN and EU levels also apply to PF (see IO.10). PF related TFS are implemented without delay (see Technical Compliance Annex R 7 and IO.10 on notification mechanisms, in particular via the consolidated national list).

829. To date, Belgium has not submitted any proposals for listing or delisting designations on sanctions lists related to UNSCRs 1718, or at the European level. This is consistent with the level of PF risk identified by Belgium. It has also not received any requests from other countries. An exemption was granted in 2019 by the SPF Finance-Treasury to allow funds transfers for three humanitarian projects in the DPRK. These transfers were monitored to ensure that the funds were not used for PF purposes.

11.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

830. The SPF Finance/Treasury was first notified in 2024 of a bank freezing assets that may be indirectly linked to the DPRK. Three transactions were identified in a case of false positives where two individuals and one non-customer entity shared the same name of designated persons, for a total amount of EUR 1 116. Verification measures by the SPF Finance are still ongoing, pending information from the Netherlands. These freezing measures, although recent and limited, appear to be consistent with the level of PF risk identified by Belgium.

831. The CTIF states that it has not received any suspicious transaction reports (STRs) on individuals targeted by PF related TFS. No cases relating to proliferation and its financing are being dealt with by the judicial authorities.

11.5. FIs and DNFBPs understanding of and compliance with obligations

832. The findings regarding reporting entities' understanding of and compliance with TF related TFS also apply to PF related TFS (see IO.10). In general, reporting entities' understanding of PF related TFS is limited to identifying potential cases of breach or non-implementation of TFS, rather than identifying more sophisticated ways of evading PF related TFS. FIs have a level of understanding of their obligations on PF related TFS that is comparable with that of TF related TFS. However, DNFBPs have a very limited understanding of their obligations and some have only a partial understanding of the definition of beneficial owner (see IO.5), which may reduce their ability to identify more sophisticated methods of evading TFS for PF, for example when non-designated persons act on behalf of or exercise indirect control over designated persons or entities. Furthermore, failures in checking the beneficial owners of DNFBPs (see IO.4) and relating to the reliability of data on beneficial ownership (see IO.5) are potential loopholes that designated persons could exploit. Only diamond dealers are aware to some extent that they can be used to evade sanctions regimes, particularly those affecting some countries from which diamonds originate. To date, DNFBPs have not frozen any financial or non-financial assets or property in relation to TFS for PF.

833. There is little support and communication from supervisory authorities specifically aimed at raising awareness and training reporting entities specifically on PF risks. The resources available focus on TFS in general or are limited to AML/CFT aspects. The ITAA has published specific guidance on counter-

[243] All UNSCRs that impose targeted financial sanctions associated with financing the proliferation of weapons of mass destruction are transposed into European law and apply directly in Belgium.

proliferation financing for accountants on its website (December 2023), while the National Chamber of Notaries provides similar guidance on its eNotariat intranet site. The CTIF publishes a summary of the main conclusions of the PF risk analysis on its website, to which the bar associations refer. The BNB and the FSMA do not have any specific materials to raise awareness among reporting entities PF related TFS, other than materials on due diligence and screening of sanctions lists in general.

11.6. Competent authorities monitoring and ensuring compliance with PF-related targeted financial sanctions

834. As with TF, SPF Finance is responsible for implementing freezing measures related to PF and monitoring compliance with the obligations of reporting entities. The AML/CFT supervisors for FIs and DNFBPs are responsible for ensuring that reporting entities have developed and implemented effective internal control procedures to comply with TFS obligations. The supervision carried out in this regard generally focuses on compliance with TFS and does not specifically target TF sanctions (see IO.10).

835. Information on the frequency and nature of supervision specifically relating to how financial institutions apply PF related TFS is not available. However, the examples that Belgium provided show that the supervision carried out by the FIs supervisors is fairly satisfactory.

836. DNFBPs supervisors have not detected breaches or non-implementation of the sanctions regime imposed on the DPRK.[244]

[244] The SPF Economy identified several cases of diamond dealers being involved in evading another sanctions regime in 2023 and 2024. These examples were reviewed by the evaluation team but do not fall within the scope of UNSCR 1718 and its subsequent resolutions. They are therefore not taken into account in the evaluation of Belgium's effectiveness.

Annex A. Technical compliance[245]

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

This technical compliance covers areas where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated 2015) (or follow-up reports with technical compliance re-ratings (dated 2018)[246] and areas where there has been a change in the FATF Standards for which the country has not previously been assessed. The reassessed areas are clearly identified under each heading.

For Recommendations not under review, pre-existing information from the country's most recent assessments is included. Such Recommendations are marked with a footnote cross-referencing the date and source of the information (i.e. the country's most recent mutual evaluation or follow-up reports with technical compliance re-ratings).

Recommendation 1[247] – Assessing risks and applying a risk-based approach[248]

R.1 has been reassessed because it was amended by the FATF in 2020 in order to extend the requirements to proliferation financing (PF) risks. The rating of Belgium was changed to compliant with this Recommendation in the 2018 Follow-up Report (Largely compliant in the 2015 MER).

Countries' Obligations and Decisions

Assessment of ML/TF risks

Criterion 1.1

The Belgian authorities are subject to an obligation to identify and assess ML/TF risks to which Belgium is exposed (Art. 68 para. 1 of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and the restriction of the use of cash, "AML Law"). Belgium adopted a national ML risk analysis in 2019, updated in 2023, and a national TF risk analysis in 2023. The competent authorities are required to take account of the supranational ML/TF risk assessments carried out by the European Commission in their national analyses (Art. 69, §1, 1°, AML Law).

---

[245] In accordance with the 5th Round Methodology, Recommendations under review, which have been analysed for this mutual evaluation, are in green.

[246] For details regarding how these Recommendations are identified, please refer to the section on Technical Compliance Review in your assessment body's Procedures or the Universal Procedures.

[247] This assessment has been carried out in accordance with the April 2024 Methodology, but the numbering of the criteria in R.1 has been adapted to the later Methodology (i.e. the references to C.1.4.a and C.1.9.a have been removed, leading to the renumbering of the following criteria, without any change in substance).

[248] R.1 has been reassessed because of the changes made by the FATF, for which Belgium has not previously been assessed.

Criterion 1.2 –

Two coordinating bodies are responsible for national risk assessments (NRAs) (Art. 68, para. 1 and 4 14°, AML Law): the Ministerial Committee for Co-ordinating Measures Against Laundering Money from Illegal Sources (Art. 3 of the Royal Decree (RD) of 23 July 2013) and the National Security Council for countering terrorism and terrorist financing (Art. 3, RD of 22 December 2020).

Criterion 1.3 –

The Belgian authorities are required to update the NRAs every two years, or more frequently if warranted by circumstances (Art. 68, para. 2, AML Law). The NRA BC was last updated in 2023, after its adoption in 2019 (c. 1.1).

Criteria 1.4 –

A mechanism has been implemented to provide information on the results of risk assessments – through representation on AML/CFT coordination bodies (mentioned in C. 1.2). The fact that certain competent authorities (National Bank of Belgium, BNB; Financial Services and Markets Authority, FSMA; SPF Economy, SPF Justice and SPF Finance) and self-regulatory bodies (c. 2.2) are not represented on the National Security Council in charge of CFT deprives them of direct access to information on the TF NRA. Nevertheless, the Belgian financial intelligence unit (FIU) known as the Cellule de traitement des informations financières (CTIF) provides this information to all authorities responsible for conducting sectoral NRAs. Companies subject to the law are provided with appropriate information on the results of NRAs (Art. 70 4° AML Law).

Assessment of PF risks

Criterion 1.5 –

(a) Belgium does not have a legal basis for the requirement to identify and assess PF risks. However, in 2024 the country adopted a national analysis of PF risks, (b) coordinated by SPF Finance - Treasury. (c) There is no requirement to update the PF national risk assessment. (d) There is no mechanism to disseminate the results of the national risk assessment.

Measures to mitigate ML/TF risks

Criteria 1.6 –

On the basis of the national ML/TF risk assessment, the Belgian authorities identify the measures to be taken in areas requiring increased vigilance and formulate recommendations to improve the allocation and prioritisation of resources (Art. 70 1° to 3°, AML Law).

Criterion 1.7 –

The following may be exempted by Royal Decree from the application of the obligations imposed on entities subject to the AML/CFT system: (a) gaming establishments whose transactions present a proven low ML/TF risk, taking particular account of the nature and scale of the transactions, as well as the payment methods used (Art. 5 §2, AML Law); (b) operators carrying out financial activities other than money transfers on a limited basis and ancillary to their main business, on the basis of an appropriate risk assessment (Art. 5 §3, AML Law). The conditions for entitlement to exemptions have been met.

Criteria 1.8 –

(a) On the basis of the national risk assessment, the Belgian authorities identify the measures to be taken in areas requiring increased vigilance (Art. 70 1° to 2°, AML Law). (b) Obliged entities are required to take account of the relevant conclusions of national risk assessments (Art. 16 para. 3, AML Law).

Criterion 1.9 –

Belgium does not organise a general scheme of simplified measures as such.

Criterion 1.10 –

The supervisory authorities monitor compliance by regulated entities with their AML/CFT obligations and issue regulations specifying technical points, taking account of the national risk assessment (Art. 85 and 86, AML Law). In addition, the competent authorities, including supervisory authorities and self-regulatory bodies, have a general obligation to take ML/TF risk assessments into account when implementing AML/CFT obligations (Art. 7, AML Law). This obligation must be combined with the requirement for obliged entities to be able to demonstrate to their supervisory authorities that the due diligence measures they apply are appropriate in light of the ML/TF risks they have identified (Art. 19 §2, para. 3, AML Law).

Measures to mitigate PF risks

Criterion 1.11 –

(a) to **(d)** - Belgium does not have a legal basis for the requirement to take measures to mitigate PF risks, nor for allocating resources effectively to mitigate those risks.

Obligations of financial institutions and designated non-financial businesses and professions

Assessment of ML/TF risks

Criterion 1.12 –

Obliged entities must take appropriate measures, proportionate to their nature and size, to identify and assess the ML/TF risks to which they are exposed, taking particular account of the characteristics of their customers, their products, services or transactions, the countries or geographical areas covered, and the distribution channels used (Art. 16, AML Law). **(a)**, **(c)** and **(d)**. These assessments must be documented, kept up to date and made available to the competent authorities (Art. 17, AML Law). **(b)** They must also take account of the factors set out in the Law as indicating a potentially lower or higher risk (Art.16 of the AML Law).

Measures to mitigate ML/TF risks

Criterion 1.13 –

Reporting entities are subject to the obligation to **(a)** define and apply effective internal control policies, procedures and measures proportionate to their nature and size (Art. 8 §1 of the AML Law), approved by a member of a high management level (Art. 8 §3, AML Law), to mitigate and effectively manage the risks identified at the level of the European Union, Belgium and the obliged entity itself (art. 8§1 1° AML Law); **(b)** to ensure the relevance and effectiveness of the measures taken and to improve them where necessary (art. 8 §4 AML Law); and **(c)** to apply increased vigilance measures when they identify higher risks (art. 19 §2, para. 2, AML Law).

Criterion 1.14 –

Reporting entities may apply simplified measures where they identify lower risks, and in doing so must generally take account of the conclusions of the national risk assessment (Art. 19 §2, para. 1 and 2, AML Law). Criteria C. 1.10, 1.12 and 1.13[249] are met. Simplified measures are not authorised in cases of suspected ML/TF which involve a suspicious transaction report, as this is a situation which precludes a finding of a lower risk situation (Art. 19 §2, para. 3, AML Law). In addition, financial institutions must re-assess the individual risks of their customers concerned in order to apply enhanced due diligence measures if necessary

[249] Text of the Methodology referring to C. 1.9 to 1.11 to be corrected because PF is to be considered in isolation. See updated version of the Methodology (August 2024).

or to terminate the business relationship (Art. 22, BNB AML Regulation of 21 November 2017 on ML and TF prevention, and Art. 23, FSMA AML Regulation of 3 July 2018 on ML and TF prevention[250]).

Assessment of PF risks and measures to mitigate them

Criterion 1.15 –

Belgium does not have a legal basis for the requirement to take measures to identify, assess and mitigate PF risks for financial institutions and for designated non-financial businesses and professions.

> *Weighting and conclusion* – Belgium has generally adequate measures for assessing ML and TF risks and applying a risk-based approach. However, there is no applicable framework for PF risks. **Belgium is largely compliant with R. 1.**

Recommendation 2[251] – National cooperation and coordination[252]

R. 2 has been reassessed because it was amended by the FATF in 2020 in order to reflect the new PF risks. The rating of Belgium was changed to compliant for this Recommendation in the 2018 Follow-up Report (Largely compliant in the 2015 MER).

Criterion 2.1 – The Ministerial Committee for Co-ordinating Measures Against Laundering Money from Illegal Sources is responsible for establishing general AML policy (Art. 3, Royal Decree (RD) of 23 July 2013). Following the adoption of the national ML, TF and PF risk analyses (C. 1. 1 and 1.5), an action plan was endorsed by the Ministerial Committee in 2024 and translated into a national policy, which focuses primarily on AML. The national AML policy also takes account of the risks identified in the analysis of TF and PF risks. However, there is no legal basis for extending the powers of the Ministerial Committee for Co-ordinating Measures Against Laundering Money to the fight against TF and PF; consequently, the most directly competent authorities for combating TF and PF have not been involved in defining this policy, as they are not formally part of the Committee (see C. 2.2).

The National Security Council is responsible for the strategic coordination of measures to counter TF and PF and is assisted by a Coordination Committee responsible for submitting proposals to the Council (Art. 3, RD of 22 December 2020).

Criterion 2.2 – The Ministerial Committee for Co-ordinating Measures Against Laundering Money from Illegal Sources is assisted by a Coordination Committee, which includes the competent authorities and constitutes a platform for cooperation and coordination (Art. 7, 9, 10 and 12, RD of 23 July 2013).

The Coordination Committee of the National Security Council is responsible for ensuring coordination, cooperation and exchanges of information on the fight against TF and PF between members (Art. 12, RD of 22 December 2020), but the CTIF, the customs authorities and SPFSPF Finance - Treasury, which is responsible for implementing asset freezes, are non-permanent members, and the representatives of the supervisory authorities of obliged entities do not sit on it, nor do the tax authorities.

Criterion 2.3 – The Ministerial Council for Coordination of the Fight against ML and the National Security Council are the two coordinating bodies for ML and TF/PF, respectively (see C. 2.1).

[250] The BNB and FSMA Regulations meet the conditions of *Enforceable means* within the meaning of the note on the legal basis of the obligations of FIs and DNFBPs and VASPs, Methodology p. 201, see the introduction.

[251] This assessment has been carried out in accordance with the April 2024 Methodology, but the numbering of the criteria in R.2 has been adapted to the later Methodology (i.e. the references to c. 2.2bis has been removed, leading to the renumbering of the following criteria, without any change in substance).

[252] R.2 has been reassessed because of the changes made by the FATF, for which Belgium has not previously been assessed.

Criterion 2.4 – The CTIF (Belgian Financial Intelligence Unit) has extensive mechanisms for operational cooperation with national AML/CFT players, for which it is released from its confidentiality obligation (Art. 83 §2 and 121 §2, AML Law). The supervisory authorities cooperate and exchange all relevant information with each other, notably in the case of inspections of obliged entities for which more than one authority is simultaneously responsible (Art. 121 §1, AML Law). In addition, cooperation protocols provide a framework for relations between the various authorities in charge of AML/CFT controls (e.g. Protocol defining the terms of cooperation and exchanges of information between the National Bank of Belgium and the Belgian Audit Oversight Board (Collège de supervision des réviseurs d'entreprises)) or with other competent authorities (protocol between SPF Finance, General Administration of the Special Tax Inspectorate, and the FSMA). Lastly, the College of Prosecutors General (*Collège des procureurs généraux*) has set up networks of experts, one of which addresses money laundering ("Ecofin"). The formal framework for cooperation on AML has yet to be defined, although the provisions of the AML Law apply with regard to targeted financial sanctions.

Criterion 2.5 – The Data Protection Authority (DPA) is responsible for monitoring the processing of personal data and ensuring compliance with the fundamental principles of personal data protection under the AML Law (Art 64 § 1/2). The AML/CFT cooperation frameworks between competent authorities generally set out the information sharing arrangements, taking account of requirements relating to personal data (see the protocol between SPF Finance, General Administration of the Special Tax Inspectorate, and the FSMA). In addition, prior advice is sought from the DPA by the Government where AML/CFT/FP legislation affects the processing and protection of personal data (EU Regulation 2016/679 on the protection of personal data, Laws of 3 December 2017 establishing the Data Protection authority (DPA) and 30 July 2018 on personal data).

> *Weighting and conclusion* – Belgium has generally adequate measures for national coordination and cooperation on ML. Responsibilities for CFT should be clarified to ensure that the competent bodies effectively define CFT strategy and policies and involve all the relevant competent authorities on an ongoing basis. Responsibilities concerning PF should also be clarified. **Belgium is partially compliant with R.2.**

Recommendation 3 – Money laundering offence[253]

R.3 has been reassessed to take account of the changes made by Belgium to the liability of legal persons (Law of 11 July 2018). Belgium was rated compliant for this Recommendation in the 2015 MER.

Criterion 3.1 – The criminalisation of ML (Article 505 of the Belgian *Code Pénal* (Penal Code – PC)) incorporates the material elements of the offence as defined in the Vienna and Palermo Conventions.

Criterion 3.2 – All crimes and criminal offences under Belgian law constitute predicate offences. This approach covers all the designated categories of predicate offences included in the FATF Glossary (Art. 505 PC).

Criterion 3.3 – Belgium does not apply the threshold method.

Criterion 3.4 – The offence of ML relates to the pecuniary benefits derived directly from the offence, as well as to the property indirectly representing the proceeds of the offence: property (defined broadly) and the assets replacing it, as well as the income derived from the investment of these benefits (Art. 42 PC).

Criterion 3.5 – Prosecution of the ML offence is not dependent on conviction for the predicate offence nor on proof of the predicate offence and of all its constituting elements; nevertheless, it must be demonstrated that the proceeds are of illegal origin (Cassation, 21 March 2006) or, at the very least, that the funds cannot originate from the defendant's official income; therefore, the illegal origin of the proceeds may be deduced

[253] R.3 has been reassessed because of the changes made by Belgium to the legal, regulatory or operational framework since the 2015 MER.

from the circumstance by which there is no credible data indicating the origin can be legal (Cassation, 17 December 2013).

Criterion 3.6 – The predicate offences to ML also extend to acts that are committed in another country where they constitute an offence and that would have constituted a predicate offence if committed on Belgian territory.

Criterion 3.7 – The offence of ML also applies to persons who commit the predicate offence ("self-laundering") (Art. 505 para. 2 PC).

Criterion 3.8 – Evidentiary law in Belgium is dominated by the principle of freedom in the furnishing of evidence. Article 505 para. 2, PC applies to natural persons who knew or ought to have known of the illicit origin of laundered assets, so that the element of intent and knowledge of the facts required to prove an offence of ML can be deduced from objective factual circumstances.

Criterion 3.9 – The penalties applicable to individuals convicted of ML are proportionate. On the scale of penalties applicable to offences in Belgium, the penalty for ML is in the upper-middle range (five years) and is equivalent to other comparable financial offences (handling stolen goods, misuse of company assets). The penalty for ML is 15 days' to 5 years' imprisonment and/or a fine of between EUR 156 and EUR 600,000 (Art. 505 para. 1 PC1). In addition, confiscation (Articles 43 et seq. PC) applies to the proceeds of the crime and may be added as an accessory penalty, which is likely to increase the deterrent effect of the penalties (see R.4). In all cases, the court also has the option of adding additional penalties such as forfeiture of certain civil rights or disqualification from holding certain offices or jobs.

Criterion 3.10 – A system of criminal liability applies to legal persons (Art. 5 PC). The principle of "decumulation" of liability was abrogated by the Law of 11 July 2018 amending the Penal Code and the Preliminary Title of the Code of Criminal Procedure, with the effect that the criminal liability of legal persons now applies without prejudice to the criminal liability of natural persons who are perpetrators of the same acts or who have participated in them. The penalties applicable to legal persons convicted of ML are set out in Art. 7 *bis* and 41 *bis* of the Penal Code (fines ranging from EUR 4 000 to EUR 960 000, special confiscation, dissolution/permanent closure, ban on carrying on business and publication of the decision). The maximum fine available is not sufficiently proportionate to sanction legal persons convicted in large-scale money laundering cases.

Criterion 3.11 – Belgium has appropriate ancillary offences to the offence of ML. Facilitating the commission of an offence and conspiracy to commit an offence may be considered as criminal participation and complicity (Articles 66, 67 and 68 of the Penal Code). Criminal conspiracy and participation in a criminal organisation that facilitates the commission of ML offences are also punishable offences (Art. 322-326 PC). Attempts are punishable under Article 51 of the Penal Code.

> *Weighting and conclusion* – Belgium does not have sufficiently proportionate financial penalties for legal persons. **Belgium is largely compliant with R.3.**

Recommendation 4 – Confiscation and provisional measures[254]

R.4 has been reassessed because Belgium has made legislative changes to the arrangements governing the Central Unit for Seizure and Confiscation (Organe central pour la saisie et la confiscation – OCSC) (Law of 4 February 2018). Belgium was rated compliant with the requirements of R.4 in the 2015 MER.

Criterion 4.1 – Belgium has a special confiscation regime, i.e. ancillary to a primary sanction, which applies in the event of conviction for any crimes or criminal offences, including ML and TF. Confiscation may be

[254] R.4 has been reassessed because of the changes made by Belgium to the legal, regulatory or operational framework since the 2015 MER.

ordered against all the perpetrators, co-perpetrators or accomplices of money laundering for the assets listed under (a) to (d) (Art. 42-1, 42-2, 42-3 43 *bis* and 43 *quater* PC). Article 42 of the Penal Code allows for the confiscation of virtual assets. Immovable property that constitutes the subject or proceeds of the crime may be confiscated. However, immovable property constituting the instrument of the crime[255] can only be confiscated in the case of drug trafficking, trafficking in human beings or organs and slum landlords, on the basis of specific provisions (Art. 4§6 of the 1921 Law, Art. 433 *novies* PC and Art. 433 *terdecies* PC).

Criterion 4.2 –

(a) Belgium specifically investigates the property assets referred to in Articles 42, point 3°, 43 *bis* and 43 *quater* of the Penal Code with a view to their confiscation.

(b) Belgium implements various types of provisional measures, such as freezing or seizure, in order to prevent transactions involving any type of property liable to confiscation (Articles 35, 35 *bis* and 35 *ter* of the Code of Criminal Investigation (CIC)). In urgent cases, OCSC judges have the power to request the freezing of assets directly for a maximum period of five days, including in the context of international cooperation (Art. 31/1 § 2, OCSC Law). The CTIF can also implement freezing measures for a period of five days (Art. 80 § 2 AML Law).

(c) Belgium can avail of measures to prevent or annul actions that jeopardise the country's ability to freeze, seize or recover assets subject to a confiscation order (Art. 15 and 21, OCSC Law of 2018). It is a criminal offence to damage property that has been confiscated or to refuse to hand over property that has been confiscated (Art. 507, PC). Seizure under criminal law precludes any civil enforcement proceedings against the seized property.

(d) The competent Belgian authorities are able to take all appropriate investigative measures (see R.31).

Criterion 4.3 – The rights of bona fide third parties are protected by law. Bona fide third parties claiming rights to the seized assets may also oppose the return of the assets to the person in whose possession they were seized. (Art. 23/1 para. 2, OCSC Act of 2018).

Criterion 4.4 – The OCSC is responsible for managing seized and confiscated assets where necessary. Its missions and operations were strengthened in 2018. In particular, the law gave the OCSC responsibility for managing virtual assets (Art. 7), strengthened the OCSC's legal basis as the centralised office for managing frozen assets and the national office for recovering assets in accordance with European legislation (Art. 5), and specified the procedures for returning assets (Arts. 19 and 23). The OCSC has the necessary powers to dispose of seized assets so that they can be managed at constant value (Art. 28 *octies*, CIC).

Weighting and conclusion – The confiscation of immovable property in the limited case in which it constitutes the instrument of a crime is not provided for in the Belgian Penal Code (PC), other than in the framework of certain specific predicate offences. **Belgium is largely compliant with R. 4.**

[255] Cour de Cassation, Cass. ruling no. P.09.0240.F, 27 May 2009.

Recommendation 5[256] – Terrorist financing offence[257]

Belgium was deemed to be largely compliant with the requirements of R.5 in the 2015 MER. R.5 was reassessed in the 2018 Follow-up Report, as a new requirement was added by the FATF to R.5 in February 2016, obliging countries to criminalise the financing of foreign terrorist fighters. R.5 has been reassessed as compliant.

Criterion 5.1[258] - Terrorist financing is addressed in Articles 140 para. 1 and 141 PC (unchanged since their introduction in 2004). Belgian positive law does not generally make FT a principal offence. Article 140 considers TF to be an act of participation in a terrorist group's activity, defined notably as the provision of information or material resources to the terrorist group, or any form of financing of a terrorist group's activity, with knowledge that such participation contributes to the commission of a crime or offence by the terrorist group (in Belgium or elsewhere). A terrorist group is defined (Article 139 PC) as a structured association of more than two persons, established over a period of time, which acts in a concerted manner with a view to committing the terrorist offences referred to in Article 137 of the Penal Code, setting out the offences referred to in Article 2(1)(b) of the International Convention for the Suppression of the Financing of Terrorism (TF Convention). a4.3. Article 141 of the Penal Code criminalises any person who, other than in the cases provided for in Article 140 of the Penal Code, provides material resources, including financial assistance, with a view to committing a terrorist offence referred to in Article 137 of the Penal Code.

Criterion 5.2 – Requirements concerning the intent and material elements of TF offences are mostly met:

- *Intent*. This element is established by the fact that the author should have known that the funds or any material resources would be used for this purpose.
- *Providing or collecting funds directly or indirectly.* Art.140 of the Penal Code criminalises the provision of material resources or any form of financing to terrorist group activity. Art.141 PC punishes the provision of material resources, including financial assistance. None of these concepts is defined in the law. The law does not introduce any restriction, i.e. funds do not have to be provided directly to constitute an offence.
- *Providing or collecting funds used with the intention of committing one or more terrorist acts* Art.140 PC stipulates that a criminalised act must contribute to the commission of a crime or a criminal offence by a terrorist group, whether or not it is qualified as a terrorist act. Art.141 PC criminalises the provision of financial assistance with the intention of committing a terrorist act.
- *Providing or collecting funds used by a terrorist organisation or by an individual* (even if there is no connection to any specific terrorist act(s)). The MER ascertained that the offence of terrorist financing did not appear to be established in the case of the provision of funds to one or two persons without proof of a link with a specific terrorist offence.

An amendment to Article 141 of the Belgian Penal Code that came into force on 1st January 2017 remedied the shortcoming identified in the MER. This new provision stipulates that anyone who provides material resources (including financial resources) to another person, with the intention of committing, or in the knowledge that this other person is committing or is going to commit, a terrorist offence defined in Art. 137, will be covered by the legislation. It is therefore not necessary to prove a link with a specific terrorist offence.

---

[256] This assessment has been carried out in accordance with the April 2024 Methodology, but the numbering of the criteria in R.5 has been adapted to the later Methodology (i.e. the references to c. 5.2bis has been removed, leading to the renumbering of the following criteria, without any change in substance).

[257] Mutual Evaluation Report (2015) and Follow-up Report (2018)

[258] R.5 is not under review, and the analysis is taken from the 2015 REM and the 2018 Follow-up Report, for which there were no sub-criterion ratings. The same applies to all other Recommendations that are not being reviewed in this mutual evaluation

In addition, the financing of terrorist offences covers the act of providing material means, including financial means, directly or indirectly, with the intention of them being used, or in the knowledge that they will be used, to commit or contribute to:

- a terrorist act as defined in Art. 137;
- the preparation of a terrorist offence (Art. 140 *septies*);
- a journey (departure from or entry into the country) by a person with the aim of committing a terrorist offence in Belgium or abroad (Art. 140 *sexies*);
- the provision or following of training in methods and techniques for committing a terrorist offence (Art. 140 *quinquies* and *quater*);
- the recruitment of persons with a view to committing a terrorist offence (Art.140 *ter*);
- dissemination of information inciting the commission of a terrorist offence (Art.140 *bis*); and
- participation in the activities of a terrorist group (Art. 140).

The scope of application is therefore very broad, covering any material action taken with a view to committing or contributing to a terrorist offence.

Criterion 5.3 – In February 2016, a new requirement was added to R.5, obliging countries to criminalise the financing of foreign terrorist fighters. Article 141 of the Belgian Penal Code, which came into force on 1st January 2017, remedied the shortcoming identified in R.5.

The financing of terrorist offences covers the act of providing material means, including financial means, directly or indirectly, with the intention of them being used, or in the knowledge that they will be used, to commit a terrorist offence or contribute to a journey (departure from or entry into the territory) by a person with the aim of committing a terrorist offence in Belgium or abroad (Art. 140 *sexies*).

Criterion 5.4 – Art. 140 PC criminalises providing material resources or any form of financing to terrorist group activity. Art.141 PC punishes the provision of material resources, including financial assistance. None of these concepts is defined in the law, but they seem sufficiently broad to cover all types of funds of illicit origin or otherwise.

Criterion 5.5 – In principle, the law does not require the funds to have been used for the offence of TF to be established. The authorities indicate that it is not necessary to have committed or to have planned to commit a terrorist offence as defined in Art. 137 PC for an offence to have occurred. With regard to the specificity of the terrorist acts financed, as indicated under Criterion 5.2, Art.140 does not, in principle, require the funds to be linked to a particular terrorist act, whereas Art.141 seems linked to a specific act. The authorities, however, indicate that the offences set forth in the Penal Code make it possible to pursue persons who provide a terrorist organisation or a terrorist acting alone, with any assistance, notably financial, without which no terrorist act would be possible. This is why there is a specific punishment applicable to persons who "aid" a terrorist organisation without knowing in advance which specific terrorist act will or will not be committed. This interpretation has not been confirmed (or invalidated) by case law concerning assistance to terrorists not acting within a terrorist group.

Criterion 5.6 – Belgian law recognises the principle of freedom in the administration of evidence. According to consistent jurisprudence from the Court of Cassation, except where the law stipulates a particular mode of proof or limits the conclusive force of a piece of evidence, the judge may base his or her beliefs on all properly obtained elements which the parties were able to freely dispute. It is therefore possible for the intent of the TF offence to be inferred from objective factual circumstances.

Criterion 5.7 – The penalties applied to the offences described in Art. 140 to 141 PC are 5 to 10 years of imprisonment and a fine of EUR 600 to EUR 30,000.[1] Accomplices to an offence are sentenced to the immediately lesser penalty, in compliance with Art. 80 and 81 PC. While the custodial sentences seem to be proportionate and dissuasive, the pecuniary penalties which are capped at EUR 30,000 do not deem dissuasive.

Criterion 5.8 – The criminal liability of legal persons under Article 2 CP applies to TF offences. The criminal sanctions applicable to legal persons are: a fine, special confiscation, dissolution, prohibition from conducting business relating to the corporate purpose, the closure of one or several sites, the publication or dissemination of the decision (Art. 7 *bis* PC). The fines applicable to legal persons range from EUR 180,000 to EUR 1,440,000 (Art. 140 Para. 1 and 141 PC). The range of applicable penalties seems relatively broad and the penalties available seem sufficiently dissuasive.

Criterion 5.9 – As a separate offence, TF is subject to the rules in the Penal Code that criminalise attempts (Article 51). The acts of complicity listed in Article 2(5) of the TF Convention are also covered by Belgian law (Articles 66 and 67 of the Penal Code on co-accomplices).

Criterion 5.10 – In Belgium, TF offences constitute ML predicate offences because Art.505 PC refers to the material benefits derived from any offence.

Criterion 5.11 – Beyond traditional territorial jurisdiction, Belgian law provides for active personality jurisdiction (*compétence personnelle active*) with regard to terrorist offences: the law applies to all persons of Belgian nationality as well as to persons whose primary residence is in Belgium (Art. 6 and 12 PC). Belgium has also stipulated its jurisdiction over terrorist offences committed abroad by non-Belgians, but only when these offences are committed against a Belgian national or Belgian institution or an institution of the EU (Art. 10 *ter* and 12 of the Belgian *Code de procédure civile* (Code of Civil Procedure – CCP).

> *Weighting and conclusion* – Belgium has implemented the new requirements of R.5 and remedied the technical shortcoming identified in the 2015 MER. **Belgium is therefore compliant with R.5**.

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing[259]

R.6 has been reassessed because Belgium has made changes to the legal framework for the application of targeted financial sanctions (TFS) in the United Nations Security Council Resolutions (UNSCRs).[260] Belgium was deemed partially compliant with the requirements of R.6 in 2015. Belgium applied for a new rating in 2018. However, the shortcomings relating to the prompt application of the targeted financial sanctions of UNSCR 1267/1989 and 1988 persisted and the partially compliant rating was maintained.

Belgium implements TF TFS through EU decisions and regulations, supplemented by national legislation.[261]

Criterion 6.1 –

(a) The SPF Foreign Affairs is the competent authority to propose the designation of persons or entities to the United Nations 1267/1989 and 1988 Committees (in accordance with the procedure established by the National Security Council for countering terrorism and TF (*Conseil national de sécurité* – CNS)). The proposal requires the agreement of the CNS (C. 1. 2) and the competent public prosecutor's office – in principle, the Federal Public Prosecutor's Office – as well as written consultation with various departments (i.e. the State Security Service (VSSE), the Central Unit for Threat Analysis (OCAM), Central Directorate for Countering

[259] R.6 has been reassessed because of the changes made by Belgium to the legal, regulatory or operational framework since the 2015 MER.

[260] Law on miscellaneous financial provisions of 2 May 2019.

[261] At EU level, UNSCRs 1267/1989 (on Al Qaeda) are implemented by Council Decision 2016/1693/CFSP and European Regulation 881/2002; UNSCR 1988 (on the Taliban) - through Council Decision 2011/486/CFSP and European Regulation 753/2011; and UNSCR 1373 was - through Council Common Position 2001/931/CFSP and European Regulation 2580/2001.

Serious and Organised Crime (DJSOC/Terro), General Intelligence and Security Service (SGRS)), and the General Treasury Administration. The CTIF is also consulted in practice and provides financial information via the OCAM database.

(b) Belgium has a mechanism for identifying individuals or entities that may be subject to UN listing adopted in December 2018 (classified decision made available to the assessment team during the on-site visit). There is no explicit requirement for targets to be identified on the basis of the criteria set out in UNSCRs 1267/1989 and 1988.

(c) Belgium has not demonstrated the application of standards of proof based on "reasonable grounds" or "reasonable basis" for proposing designations to the 1267/1989 and 1988 Committees. Belgium refers to the criteria applicable for inclusion on the national list under UNSCR 1373 (Circular of 7 September 2015 [262] and Art. 3 AR 2006). However, this Circular makes inclusion on the national list conditional upon the existence of a criminal proceeding (police or judicial investigation for terrorism), which does not comply with the requirements of criterion C. 6.1(c) in the case of designations to the United Nations Sanctions Committees.

(d) Belgium has not demonstrated that the competent authorities follow the procedures and forms provided by the UNSCRs. As Belgium has not made a proposal for designation since December 2002, it has not had to put into practice the procedures and standard forms for listing adopted by the 1267/1989 or 1988 Sanctions Committees.

(e) Belgium has not demonstrated that the competent authorities provide as much relevant information as possible in support of designation proposals to the Committees. Belgium has not stated whether it publishes its status as a State proposing designation.

Criterion 6.2 –

(a) *At the EU level*, the EU Council (through the Council's Working Party on the Application of Specific Measures to Combat Terrorism (COMET)) is responsible for designating persons or entities that meet the criteria set forth in UNSCR 1373. Designations are considered based on proposals submitted by EU member states or third states. (EU Regulation 2580/2001, art.2(3); CP 2001/931/CFSP, art.1(4)). Relevant designations of EU internals (i.e., natural persons who have their roots, main activities, and objectives within the EU) only trigger enhanced police and judicial cooperation. (CP 2001/931/CFSP footnote 1 of Annex 1). *At the national level*, the CNS is responsible for proposing the adoption of asset-freezing measures to the Council of Ministers, where measures have not already been taken at EU level (Art.3, Royal Decree (RD) of 28 December 2006). Belgium states that the CNS has the capacity to propose designations for national listing under UNSCR 1373 on the basis of requests from another country although this is not expressly provided for in the Royal Decree. This has not yet been the case in practice, as no formal requests have been submitted to Belgium.

(b) *At the EU level*, proposals for listings are made by member states (for proposals based on decisions taken by their own competent authorities), or by member states or the High Representative for Foreign Affairs and Security Policy (HR) for proposals on the basis of decision(s) by third States' competent authorities. The EU (through COMET WP) applies designation criteria consistent with the designation criteria of UNSCR 1373 (CP 2001/931/CFSP, art.1(2) & (4); CR 2580/2001, art. 2 (3), COMET WP mandate, practical arrangements and working methods 10826/1/07 REV`1)*At the national level*, targets are identified by the Central Unit for Threat Analysis (OCAM), which forwards its proposals to the National Security Council (CNS) after consultation with the judicial authorities. The CNS is then responsible for forwarding proposals to the Minister of Finance, who submits them to the Council of Ministers for inclusion on the national list.

(c) *At the EU level*, the European External Action Service or relevant member state (acting as intermediary) when receiving a request for designation from a non-EU country, will carry out a first basic scrutiny of the

[262] Circular from the Ministry of Justice and the Ministry of Finance on the implementation of the Royal Decree of 28 December 2006.

proposal and gather relevant information, including requesting additional information from the requesting country, in particular with regard to and respect for fundamental rights. (CP 2001/931/CFSP, art. 1(2) and (4), as well as COMET WP mandate, practical arrangements and working methods). If an EU country requests an EU designation, the compliance with due process is assumed when the EU reviews such requests. COMET has 15 days to review the proposal, this timeframe can be shortened in exceptional cases. (doc.14612/1/16 REV 1 on establishment of COMET WP, Annex II, arts.8-9).

At the national level, Belgium has set up a mechanism described in the "TF Handbook to assist practitioners in their implementation of UNSCR 1373", which was assessed during the 2018 Follow-Up Report. Requests follow the same procedure and decision-making mechanism as for the inclusion, removal or retention of a person or entity on the national list. This procedure was validated by the CNS in 2017.

(d) *At the EU level*, when deciding on a proposal, COMET decides on the basis of a decision (and the information/material supporting that decision) by a competent national body, irrespective of criminal proceedings (CP 2001/931/CFSP, art.1(4)).

At the national level, the requirements for deciding to designate on the Belgian national list are more restrictive than the existence of "reasonable grounds" or a "reasonable basis". Proposals for designation are conditional on the existence of judicial proceeding, and only behaviour constituting criminal offences can lead to designation. (Art. 2 and 3 of the Royal Decree of 28 December 2006 and the Circular of 7 September 2015) Freezing measures apply to persons and entities that commit, attempt to commit, facilitate or participate in terrorist offences (...). The Royal Decree therefore refers to the concept of "terrorist offence" rather than "terrorist act", as provided for in UNSCR 1373, which restricts the scope of potential targets for freezing measures and constitutes a failure to satisfactorily apply the TFS.

(e) *At the EU level*, there is no procedure or requirements regarding the provision of identifying or supporting information with respect to requesting non-EU countries to give effect to EU designations. Information to support designation may be shared with non-EU members upon request provided EU member states agree.

At the national level, Belgium has not developed a formal mechanism for requesting that another country give effect to freezing measures initiated at Belgian level and which would require Belgium to provide information and supporting evidence to the competent foreign authorities.

Criterion 6.3 –

(a) *At the EU level*, all member states are required to provide each other with all available relevant information to identify persons meeting the criteria for designation (CP 2001/931/CFSP, art.4; EU Regulation 2580/2001, art.8; EU Regulation 881/2002, art.8)

At the national level, OCAM has the power to gather and request relevant information held by the support services. This information can be used to identify individuals and entities that meet the designation criteria. (Art. 6, Law of 10 July 2006 on threat analysis, Circular of 7 September 2015).

(b) *At the EU level*, designations take place without prior notice (EU Regulation 1286/2009, preamble para.5).

At national level, there is no explicit provision for ex parte intervention against a person or an entity subject to a freezing measure. However, the Circular of 7 September 2015 suggests that persons subject to designation on the national list under RSCNU1373 would not be notified prior to their designation (section D).

Criterion 6.4 –

At the EU level, At the EU level, implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not occur "without delay.".[263] For TFS under the UNSCR 1373 mechanism, these measures are implemented without delay, except in respect of EU nationals. New designations are published on the day they are adopted and enter into force on the same day. Once the decision to freeze has been taken, European Regulation 2580/2001 is immediately applicable within all EU member states.

At the national level, Belgium has adopted a provision that remedies this shortcoming by providing for the applicability of designations in Belgium from the moment of their adoption by the UN and the Sanctions Committees (Art. 236, Law of 2 May 2019).

The TFSs linked to UNSCR 1373 at European level are implemented by European Council Regulations (in application of Regulation 2580/2001). EU Regulations, including European Council Regulations, are directly applicable in Belgium; they come into force as soon as they are adopted and simultaneously published in the Official Journal of the EU (OJEU). The freezing measures decided at national level apply immediately from the day of their publication in the *Moniteur belge* (Art. 2 of the Royal Decrees amending the composition of the national list).

Criterion 6.5 –

(a) *At the EU level,* for 1373 designations, there is no requirement to freeze assets of listed individuals that are EU internals Listed EU internals are only subject to increased police and judicial cooperation among members (CP 2001/931/CFSP footnote 1 of Annex 1). Under UNSCRs 1267/1989, 1988, 1373 all natural and legal persons within or associated with the EU are required to freeze without prior notice and delay the funds or other assets of designated persons and entities. (EU Regulation 753/2011, arts.3, 14; EU Regulation 881/2002, arts.2(1), 11; EU Regulation 2580/2001, arts.2(1)(a), and 10).

At the national level, Belgium remedies this shortcoming: Article 2 of the Royal Decree of 28 December 2006 provides for the freezing of the funds and economic resources of the persons and entities covered by the European regulations (including the EU nationals listed therein), and Article 3 applies to persons who are not covered by the European mechanisms but who are nevertheless included in a list drawn up by the CNS. Failure to comply with the obligation to freeze funds at European level is punishable by administrative and criminal penalties (Art.3 of the Law of 13 May 2003)[264] and at national level under UNSCR 1373 (Art. 4 of the Law of 11 May 1995).[265]

(b) *At the EU level*, freezing actions for UNSCRs 1267/1989 and 1988 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, or by a third party acting on their behalf or at their direction. This extends to interest, dividends or other income on or value accruing from or generated by assets (EU Regulation 881/2002, arts.1(1), 2; EU Regulation 753/2011, arts.1(a), 3). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35).

Under the EU mechanism on UNSCR 1373, the freezing obligation applies to all funds, other financial assets and economic resources belonging to, or owned or held by the designated person or entity (EU Regulation 2580/2001, arts.1(1), 2(1)). There is no explicit reference to funds or assets controlled by, indirectly owned by, derived from assets owned by, or owned by a person acting at the direction of a designated person or

[263] This is due to the time taken to consult between European Commission departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages. Though expedited procedures allow for implementation within 72 hours where possible, this does not meet the requirement of "without delay".

[264] Law on the implementation of restrictive measures adopted by the Council of the EU against States, certain persons and entities.

[265] Law on the implementation of decisions of the United Nations Security Council

entity. However, this gap is largely addressed by the EC's ability to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, art.2(3) (iii) and (iv)). As above, the notion of joint-ownership is not explicitly covered, although this interpretation is taken in non-binding EU Best Practices (EC document 8518/18, para.35).

At national level, Belgium has not taken any measures to extend the scope of the freezing obligation for designations covered by UNSCR 1373, which is still not sufficient to cover all the funds referred to in R.6 (Royal Decree of 28 December 2006).

(c) *At the EU level*, natural and legal persons are prohibited from making funds, other assets or economic resources available unless authorized by a national competent authority (EC Regulation 881/2002, art.2(2), (3); EU Regulation 753/2011, art.3(2); EU Regulation 2580/2001, art.2(1)(b)). The EU UNSCR 1373 mechanism explicitly extends to the provision of financial services (EU Regulation 2580/2001, art.2(2)). While there is no similar explicit prohibition in the EU UNSCR 1267/1989 and 1988 mechanism, this is covered by the broad definition of funds and other assets (economic resources) and the prohibition to make available assets that can be used to obtain such services (EU Regulation 881/2002, art.1(2); EU Regulation 753/2011, art.1(c)). However, deficiencies in respect of freezing obligations noted under c.6.5(a) for EU internals applies to this criterion.

EU nationals are not subject to the freezing measures set out in Regulation 2580/2001[266] but are covered by national provisions (see Criterion 6.5 (a)). The Royal Decree of 28 December 2006 (Art.4) prohibits making funds or economic resources available to persons or entities listed at European level or in Belgium in accordance with the obligations of R.6.

(d) At the EU level, information on EU designations is published in the Official Journal of the EU, and included in the EU's Financial Sanctions Database the next working day (which includes a newsletter service to which FIs and DNFBPs can subscribe), though there may be delays to updates via the newsletter service notably in case of designations on Fridays or over the weekend. Guidance in relation to EU sanctions is published on the website of the European Commission.

At the national level, SPF Finance maintains a consolidated list of national and European designations that can be accessed on its website, which features a notification system for persons and entities that have subscribed to it, enabling them to be informed of changes to the consolidated national list. This list is sometimes not updated immediately when a UN designation has been made just before a weekend or public holiday. However, publication on this list does not constitute legal grounds for implementing the freezing measures under UNSCR 1267/1989, 1988 and subsequent resolutions. As these are directly applicable in Belgium, this mitigates the impact of these delays. SPF Finance website also contains general information about TFS and brief, general instructions on freezing obligations. Belgium has not provided any guidelines for obliged entities (with the exception of a guide for diamond dealers in 2021 which is no longer up to date) and any other persons vis-à-vis their freezing obligations (apart from general information on the SPF Finance website).

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations to their respective national competent authorities. This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations. The scope gap in obligations in respect of 1373 designations (EU internals) also applies to this criterion. (EU Regulation 753/2011, art.8; EU Regulation 881/2002, art.5(1); EU Regulation 2580/2001, art.4).

[266] EU nationals are persons whose origin, main activities and objectives are located in the EU (Art. 4 of CP 2001/931/CFSP and footnote 1 of the Annex).

At the national level, FIs and other persons and entities must report the assets frozen to SPF Finance and the measures taken in accordance with the bans of the relevant UNSCRs (Art. 8 RD 28 December 2006). This obligation does not explicitly extend to the reporting of attempted transactions.

(f) *At the EU level,* for 1267/1989, 1988 and 1373 designations, third parties acting in good faith are protected (EU Regulation 753/2011, amended by EU Regulation 1286/2009, and 2016/1686 art. 12 and 13, art.6 and 7; EU Regulation 881/2002, art.6; EU Regulation 2580/2001, art.6).

Criterion 6.6 – Procedures are published in the EU and Belgian Official Journals for the delisting and the unfreezing of funds of persons or entities that no longer meet the designation criteria.

(*a*) *At the EU level*, for designations under the 1267/1989 and 1988 mechanisms, there are procedures to submit de-listing requests to the relevant UN Sanctions Committee in line with Committee procedures (EU Regulation 881/2002, art.7c; EU Regulation 753/2011, art.11(4)). EU measures imposing targeted financial sanctions pursuant to 1267/1989 and 1988may be challenged by instituting proceedings before the EU Court of Justice (art.263, par.4 and art.275, par.2 of the Treaty on the Functioning of the European Union for challenging EU regulations or CFSP Decisions). *At the national level*, delisting requests are coordinated by the Ministry of Foreign Affairs and its representative at the UN or via the European Commission.

(b) *At the EU level*, de-listing procedures are available for designations under the 1373 mechanism under EU Regulation 2580/2001

At the national level, Art.5 of the RD of 28 December 2006 establishes a procedure for requesting removal from the Belgian list. Each delisting request must be submitted to the Minister of Finance, which forwards the request without delay to the CNS for examination within 30 days. During the examination, the CNS may ask OCAM to update its assessments. The CNS then sends a proposal to maintain or delist a name, or to add information for approval by the Council of Ministers

(c) *At the EU level,* a person or entities designated under the 1373 mechanism can write to the EU Council to have the designation reviewed by COMET WP (CP 2001/931/CFSP) or may institute a proceeding before the EU Court of Justice (Treaty on the Functioning of the European Union, arts.263(4), 275(2)). *At national level*, ordinary law applies: the designation decision is an administrative decision that can be challenged before the Belgian courts.

(d) and **(e)** *At the national level,* for designations pursuant to UNSCR 1267/1988 and 1989, designated persons and entities are notified of their designation and of the reasons for it and legal consequences by the CNS. They also have the right to request a review of the designation decision in court. *At the EU level*, persons designated under UNSCR 1267 etc. and 1988 are informed of applicable de-listing procedures, which include the availability of the focal point (for designations under UNSCR 1989) and the UN Office of the ombudsperson (for UNSCR 1267/1989 designations). (EU Regulation 881/2002, art.7(a); EU Regulation 753/2011, art.11(4)).

(f) *At the EU level*, procedures for unfreezing funds due to cases of mistaken identity are in place (EC document 8519/18, paras.8-17, 37). *At national level*, persons erroneously affected by a freeze mechanism may request the unfreezing of funds through the procedures described in C. 6.6 (a) to (e), which apply to the unfreezing of funds or other property of persons or entities with the same or a similar name to that of the designated persons or entities. These procedures can be consulted on the SPF Finance website.

(g) *At the EU level,* de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c.6.5.d) also contains information on the obligations to respect a delisting action. *At national level,* decisions on removal from the Belgian list and on the unfreezing of funds are published in the Belgian Official Journal.

Criterion 6.7 – *At the EU level,* the regulations imposing TFS obligations contain measures for national competent authorities to authorise access to frozen funds, where necessary for basic expenses or the payment of certain expenses in line with UNSCR 1452 (EU Regulation 881/2002, art.2a; EU Regulation 753/2011, art.5; EU Regulation 2580/2001, arts.5, 6). Procedures are also in place *at national level* to authorise access to frozen funds or other assets deemed necessary to cover basic expenses and the payment of certain types of charges, or for extraordinary expenses (Art. 6 RD 28 December 2006).

> ***Weighting and conclusion*** – A mechanism is in place to implement targeted financial sanctions in accordance with United Nations Security Council Resolutions 1267/1989 and 1988. However, there are shortcomings in the procedures and criteria for identification and designation under UNSCR 1267/1989 and 1988. With regard to UNSCR 1373, Belgium applies criteria that limit the identification of potential targets to cases in which that person/entity is the subject of a police or a judicial investigation. This factor weighs heavily in the rating of this Recommendation, as it restricts the wider use of targeted financial sanctions as a preventive tool to deprive terrorists, terrorist organisations and persons who finance terrorism of the resources and means to finance or support terrorist activities and organisations. Furthermore, Belgium has not developed a mechanism for requesting another country to give effect to freezing actions initiated at the Belgian level. **Belgium is partially compliant with R.6.**

Recommendation 7 – Targeted financial sanctions related to proliferation[267]

Recommendation 7 has been reassessed because Belgium has made changes to the legal framework for the application of UNSCR targeted financial sanctions since its 2018 Follow-Up Report. Belgium was rated partially compliant with the requirements of R.7 in the 2015 MER. Belgium applied for a new rating in 2018. However, the shortcomings relating to the prompt application of targeted financial sanctions for proliferation financing persisted and the partially compliant rating was maintained.

Belgium relies mainly on European legislation to implement R.7.[268] Currently, the relevant UNSCRs in force are Resolution 1718 concerning the Democratic People's Republic of Korea (DPRK) and its subsequent Resolutions 1874, 2087, 2094, 2270, 2321 and 2356. In European law, these Resolutions are transposed by European Regulation 2017/1509.[269]

Criterion 7.1 – *At the EU level*, At the EU level, implementation of TFS, pursuant to UNSCR 1718, does not occur "without delay." This is due to the time taken to consult between European Commission departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages. To address this shortcoming Belgium, adopted a provision at national level that provides for the applicability of designations in Belgium from the moment of their adoption by the UN (Art. 236, Law of 2 May 2019).

Criterion 7.2 – The Treasury Administration within SPF Finance is responsible for implementing targeted financial sanctions related to proliferation.

(a) *At the EU level*, all natural and legal persons within the EU are required to freeze the funds or other assets of designated persons or entities as soon as a designation is published, i.e. without prior notice (EU Regulation 2017/1509, art.1and 2). Though delays in implementation apply as described under c.7.1. The

[267] R.7 has been reassessed because of the changes made by Belgium to the legal, regulatory or operational framework since the 2015 MER.

[268] All UNSCRs that impose targeted financial sanctions in connection with the financing of the proliferation of weapons of mass destruction have been transposed into European law and are directly applicable in Belgium.

[269] The TFS relating to the Islamic Republic of Iran set out in UNSCR 2231 ceased to apply on 18 October 2023 and are therefore not assessed in this report. The TFS provisions of UNSCR 1737 and successor resolutions have subsequently been re-applied (on 27 September 2025), but they are not covered in this assessment as this occurred after the end of the on-site period in January – February 2025.

provisions described in c.7.1 allow for the implementation of TFS without delay (see C. 7.1). At national level, the provisions of Articles 236 and 237 of the Law of 2 May 2019 provide for the immediate implementation and enforcement, without prior notice, of freezing measures adopted under the UNSCR, including in relation to FP, and sanctions are foreseen in case of failure.

(b) *At the EU level*, freezing actions for UNSCR 1718 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, and includes assets generated from such funds. (EU Regulation 2017/1509, art. 1 and 34). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35). While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds 'controlled' by the designated person (Para 55b. of the Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy) These concepts are not clarified more explicitly by national provisions.

(c) *At the EU level*, EU nationals and natural and legal persons within the EU are prohibited from making funds and other assets available unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU regulation 2017/1509, art.34(3)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU.

(d) At the EU level, the same mechanism to communicate PF TFS is used for TF TFS (c. 6.5 d). *At national level*, the consolidated list of national and European designations maintained by SPF Finance and published on its website includes PF designations. However, communication through this list is not always immediate when a UN designation has been made just before a weekend or public holiday. This website also contains general information about TFS and brief, general instructions on freezing obligations. However, Belgium has not provided more specific guidance to FIs, DNFBPs and others on their specific freezing obligations in the context of targeted proliferation-related financial sanctions (apart from general information on the SPF Finance website)

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations. (EU Regulation 2017/1509, art. 50). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations. *At national level*, FIs and other persons and entities must report the assets frozen to SPF Finance and the measures taken in accordance with the bans of the relevant UNSCRs (Art. 8 RD 28 December 2006). It is not clearly stated that attempted transactions must be declared.

(f) At the EU level, protections are in place for third parties acting in good faith (EU Regulation 2017/1509, art.54)

Criterion 7.3 – Since the AML Law came into force in 2017, obliged entities have been required to adopt adequate organisational procedures, policies and internal control measures to comply with financial embargo obligations, either asset freezing or other restrictive measures, and due diligence duties in this field (Art. 8). The supervisory authorities are responsible for ensuring compliance with the obligations set out in R7. SPF Finance is competent to impose penalties in the event of non-compliance (Art. 85 and 132 AML Law and Art. 7 Law of 13 May 2003[270]). Administrative and criminal penalties are imposed for failure to comply with anti-proliferation obligations, i.e. imprisonment of between eight days and five years and a fine of between EUR 25 and 25,000 in the criminal sphere and a fine of between EUR 250 and 2.5 million in the administrative sphere (Art. 6, Law of 13 May 2003).

[270] Law of 13 May 2003 – Law on the implementation of restrictive measures adopted by the Council of the European Union against States, certain persons and entities.

Criterion 7.4 –

(a) *At the EU level*, listed persons are informed of their ability to petition the UN Focal Point or their own government for de-listing, through the EU Best Practices document for the effective implementation of restrictive measures (page 11, para. 23). *At the national level*, information and links explaining how the procedures operate are available to the public on the SPF Finance website, which is the focal point in accordance with UNSCR 1730.

(b) *At the EU level*, procedures for unfreezing funds due to cases of mistaken identity are the same as those described under c.6.6(f). Similarly*, at the national level*, persons erroneously affected by a freeze mechanism may request the unfreezing of funds through the same procedures described in C. 6.6 to (e), which apply to the unfreezing of funds or other property of persons or entities with the same or a similar name to that of the designated persons or entities. These procedures can be consulted on the SPF Finance website.[271]

(c) *At the EU level,* the regulation imposing TFS obligations under UNSCR 1718 contains measures for national competent authorities to authorise access to frozen funds or other assets under the conditions set out in UNSCR 1718. (EU Regulation 2017/1509, art. 35-36). *At the national level*, SPF Finance is the competent authority to grant exemptions from financial penalties upon request. The procedure is set out on its website.

(d) The same mechanisms described in c.6.6 (g) apply to the communication of delisting decisions and the unfreezing of funds in relation to PF. *At the EU level*, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c7.2(d) also contains information on the obligations to respect a de-listing action.

Criterion 7.5 –

(a) At the EU level, t the EU level, regulations permit the addition of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures. (EU Regulation 2017/1509, art. 34(9)).

(b) This sub-criterion is not applicable, as the TFS elements of UNSCR 2231 expired on 18 October 2023. Therefore, this analysis did not assess the implementation of UNSCR 2231.

> *Weighting and conclusion* – Belgium relies mainly on the European framework for implementing targeted financial sanctions for proliferation financing. There are minor deficiencies relating to the updating of the consolidated national list when a UN designation is made just before a weekend or public holiday, the absence of an explicit obligation to report attempted transactions to the SPF Finances, and the lack of targeted instructions on FP related SFC. **Belgium is largely compliant with R.7**.

[271] https://finance.belgium.be/en/control-financial-instruments-and-institutions/compliance/financial-sanctions/cases-homonymy

Recommendation 8 – Non-profit organisations (NPOs)[272]

R.8 has been reassessed following the FATF's clarification of the requirements and the reform of the legal framework applicable to NPOs in Belgium with the entry into force of the Code of Companies and Associations (CSA) in May 2019. The CSA applies to all Belgian NPOs: public interest foundations (FUP), private foundations (FP), non-profit organisations (Associations sans but lucratif, ASBL) and international non-profit organisations (Associations internationales sans but lucratif, AISBL). Existing NPOs had until 1st January 2024 to adapt their articles of association.

R.8 had been assessed as partially compliant in REM 2015. The identified shortcomings concerned information and awareness-raising initiatives for the NPO sector on TF risks, the scope of controls, which did not cover all the required elements, and the lack of proportionality in the applicable penalties. R.8 was reassessed in the 2018 Follow-Up Report and rated as largely compliant.

Criterion 8.1 –

(a) At the end of 2024, Belgium had almost 144,505 NPOs, of which approximately 2,493 have been identified as falling under the FATF definition. These are primarily NPOs that have applied for approval for tax-reduction purposes. As of 30 July 2024, there were 2,449 such NPOs (including 2,323 ASBLs, 67 FUP and 15 FP), in addition to 93 NPOs operating abroad with public funding, often in high-risk areas. Applying to SPF Finance for approval is not compulsory. It is a voluntary approach, generally motivated by the desire to give donors a tax break: a 45% tax reduction for cash donations of EUR 40 or more. Belgium considers that this tax incentive is particularly attractive for NPOs whose main activity is the collection and redistribution of funds. The current list of 2,493 approved NPOs appears to include a large majority of Belgian NPOs corresponding to the FATF definition, but it is not exhaustive, as the approval process is purely voluntary. Some NPOs – despite meeting the FATF definition of an NPO – may choose not to apply for approval, notably to avoid being identified or subjected to the oversight applied to approved NPOs. This constitutes a limitation in the system for identifying NPOs potentially posing a TF risk.

(b) Belgium has carried out two TF assessments, in 2020 and 2023 (c.1.1), in addition to a specific evaluation of NPOs in 2019, updated in 2024 (SPF Justice), with contributions received from organisations including the police, justice, CTIF, SPF Economy and SPF Finance, and the State Security Service. NPOs identified as posing significant TF risks include: NPOs which are active abroad and in high-risk areas (TF through humanitarian aid), religious NPOs with extremist aims and/or run by individuals with extremist views; dormant NPOs, and those linked to illicit financial transfers conducted outside the financial system. However, the number of NPOs per category is not clearly defined. This lack of accurate data makes it impossible to determine the nature of the FT risks faced by NPOs in Belgium, and therefore also means that measures cannot be targeted at the NPOs most vulnerable to TF risk (see analysis below).

Belgium has additional measures in place to regulate certain categories of non-profit organizations (NPOs), particularly those active in development cooperation and operating abroad (see criterion 8.3). However, limitations remain in identifying NPOs at risk of terrorist financing. In the absence of a comprehensive mapping of registered NPOs, it is not possible to confirm that the above-mentioned additional measures are effectively applied to the most exposed entities.

(c) Belgium has general measures in place to regulate the non-profit sector, particularly regarding transparency, governance, and oversight. However, these measures are not specifically designed or

[272] R.8 has been reassessed due to changes made by the FATF for which Belgium was not previously assessed.

implemented based on the identified TF risks (see c. 8.3). The lack of a targeted, risk-based approach to TF represents a significant shortcoming with respect to c. 8.1(c).

Criterion 8.2 –

(a) Increased transparency of NPOs and greater public confidence in the not-for-profit sector have been reasons for the reform of the NPO framework, which is now aligned with that of companies (introduction of the CSA).

(b) The Belgian authorities have introduced a number of awareness-raising initiatives aimed at NPOs in order to prevent risks of exploitation for TF purposes. In particular, SPF Justice has organised information days, with a specific component in 2024 for NPOs linked to cults and philosophical organisations. SPF Finance also ran information sessions on targeted financial sanctions and beneficial owner obligations. In June 2024, an awareness-raising letter was sent to NPOs (as defined by the FATF), representatives of religious denominations and NPOs active in development cooperation. An inter-SPF (Justice, Economy, Finance) webinar was also organised in December 2024 to reinforce this targeted communication.

(c) Belgium maintains a dialogue with the non-profit sector, notably through its federations. Dialogue is also maintained between SPF Justice (agency for religious denominations and secularism) and representatives of recognised religious denominations and non-denominational organisations or those in the process of obtaining recognition. The Dialogue Council[273] provides an opportunity to discuss sensitive issues, including financial management, which may indirectly contribute to TF risk management. The Advisory Committee for the Cohesion of Cultures and Nations (*Comité Consultatif pour la Cohésion des Cultures et des Nations* – CCCNG) also facilitates exchanges with NPO federations and organised an AML/CFT awareness-raising session in February 2024. In addition, representatives of the NPO sector meet with FEBELFIN (representatives of the financial sector) to discuss AML/CFT obligations and the specificities of the NPO sector, with a view to developing appropriate best practices. Meetings are also held with SPF Finance, SPF Economy and SPF Justice, to reinforce consultation and prevent abuses.

(d) The Belgian authorities regularly remind NPOs of the importance of using regulated financial channels, particularly through awareness-raising initiatives by SPF Justice and SPF Finance, as well as on their websites. For NPOs active in development cooperation and receiving public subsidies, the obligations are aligned with IATI standards, which make traceability a requirement for all financial transfers (Royal Decree of 11 September 2016). In addition, all NPOs are required to state their bank account number when they register with the *Banque-Carrefour des Entreprises* (Article III.18, §1, 11° of the Belgian Code of Economic Law (CDE) (see R.24).

Criterion 8.3 – **(a) and (b)** Numerous general measures, laws and regulations exist to enhance g the transparency, governance, and functioning of the NPO sector. While this framework can , in principle, help mitigate TF risks, these measures are not specifically designed based on TF risks, nor grounded in an analysis aimed at identifying and monitoring the NPOs most exposed to such risks. These measures include:

- the obligation to provide information on beneficial owners: NPOs must collect, keep and transmit adequate, accurate and up-to-date information on their beneficial owners in the UBO register (Article 1:35 CSA, see R.24). However, certain limitations have been identified in the system (see C.24.8 and RI.5).
- increased governance and financial control requirements: Large NPOs[274] are required to have their accounts audited by a statutory auditor (Art. 3:47, § 6, CSA). NPOs active in the field of non-

[273] Convened twice a year, the Dialogue Council brings together representatives of recognised religious denominations, organised secularism (the only non-denominational organisation currently recognised), the Minister of Justice, the Prime Minister and FPS Justice. Buddhism, which is in the process of obtaining recognition, has recently been included.

[274] An NPO is considered to be "large" if it exceeds more than one of the following three criteria at the balance sheet date: 1) an annual average of more than 50 full-time equivalents; 2) annual turnover in excess of EUR 9 million; 3) a balance sheet total in excess of EUR 4.5 million (Art. 1:28, §1, CSA).

governmental cooperation and wishing to obtain accreditation to benefit from subsidies must, regardless of their size, appoint a company auditor (Article 26, §1, 4° of the Law of 19 March 2013). In addition, the annual audit of accounts by the general meeting (Article 9:12 CSA) helps to prevent misappropriation of funds and facilitates the detection of financial anomalies.

- implementation of the JustBan register (since May 2023): This register is designed to prevent abuses by ensuring that people appointed as directors of NPOs are not disqualified from managing a legal entity.

Other measures contribute to regulating certain categories of NPOs which are potentially exposed to TF risk, although they are not specifically designed on the basis of a TF risk analysis. Controls may target internationally active NPOs or those with an extremist ideology, notably via SPF Justice[275] and the security services (pursuant to Articles 7 and 8 of the Organic Law of 30/11/1998). NPOs subsidised within the framework of development cooperation are subject to legal controls governing the use of funds, carried out by SPF Foreign Affairs and approved statutory auditors, including audits and evaluations.[276] Dormant NPOs are subject to delisting or dissolution procedures in the event of inactivity. To limit financial exclusion, a basic banking service has been introduced and an across-the-board audit of the National Bank of Belgium (BNB) has been carried out (see details in IO.10). However, these schemes are based on administrative or sectoral criteria, rather than on the targeted identification of NPOs at high risk of TF. Consequently, some potentially vulnerable entities, such as NPOs involved in international cooperation and humanitarian aid without public funding, are not covered by specific monitoring measures.

Criterion 8.4 –

(a) The oversight of NPOs takes place within the broader counter-terrorism framework and relies on information sharing between competent agencies within local coordination platforms (Joint Intelligence Centre and Joint Decision Centre – see IO.9). However, there is no dedicated mechanism or specific targeting system for NPOs exposed to TF risk. This limits the authorities' ability to ensure consistent monitoring of NPO compliance with targeted, proportionate, and risk-based TF measures, as well as to effectively detect high-risk entities where applicable.

Among the controls with potential relevance to TF, one is the monitoring of the implementation of targeted financial sanctions (Article 5 of the Law of 11 May 1995 and Article 7 of the Law of 13 May 2003, see R.6) by SPF Finance. However, the vast majority of these controls are primarily focused on governance, transparency, and tax compliance, and have a broader scope than measures specifically targeted at TF risk as required under c. 8.4(a). These include, inter alia: verification of financial flows and compliance with cash payment restrictions by SPF Economy; verification of BO information by SPF Finance (Article 74 §2 CSA), in line with Article 73 of the AML Law; publication of annual accounts and accounting audits of large NPOs (Articles 3:47 and 3:51 CSA); and formal verification of incorporation or statutory amendment documents (Royal Decree of 29 April 2019) by court registries to ensure legal compliance, without substantive review.

(b) Authorities have a range of sanctions applicable to NPOs or to persons acting on their behalf in cases of non-compliance with legal obligations. These include:

- in the event of failure to comply with UBO obligations: fines of between EUR 50 and EUR 5,000 for failure to keep information on beneficial owners (Art. 1:36 of the CSA), and between EUR 250 and EUR 50,000 for failure to comply with UBO registration obligations (Art, 132, § 6 AML Law). The fines incurred enable the sanctions to be tailored to the seriousness and duration of the non-compliance, ensuring a degree of proportionality. While the maximum fine of EUR 50,000 may be a very heavy

[275] FPS Justice exercises control over the paid staff of recognised local religious communities, but not directly over any NPOs linked to them; these NPOs remain subject to the general rules of the Company Code and the legislation in place.

[276] Art. 121-124 of the Law of 22 May 2003 (control of subsidies), Art. 26, §1, 4° of the Law of 19 March 2013 (statutory auditor), and Arts. 36, 47 and 49 of the Royal Decree of 11 September 2016 (justification, audit, monitoring).

burden for NPOs with average or low budgets, it seems insufficient for large NPOs with annual budgets often amounting to several hundred million EUR or more (see IO.10);

- for inaccurate information or failure to comply with UBO formalities: deregistration (Article III.42, §1, para. 6 of the CDE); and judicial dissolution for non-compliance with legal or statutory obligations, or for activities inconsistent with the objectives of the NPO (Articles 2:113 and 2:114 of the CSA). These are very severe measures, but not explicitly linked to TF risks.
- failure to comply with targeted financial sanctions: imprisonment of between 8 days and 5 years and a fine of between EUR 250 and EUR 2,500,000 may be imposed (Art. 4 of the Law of 11 May 1995 and Articles 233 and 237 of the Law of 2 May 2019);
- in the case of TF by an NPO: the natural persons involved face the penalties set forth in Articles 140 and 141 of the Criminal Code (see R5 - C.5.7), while a non-profit association (the type of NPO most often involved in FT), as a legal person, may be fined in accordance with these same articles;
- if a legal person is convicted, the penalties are set forth in Articles 35 to 37 of the Criminal Code (winding-up: if the legal person was intentionally created or misused for criminal activities, followed by its liquidation; temporary or permanent ban on carrying out activities related to its corporate purpose; temporary or permanent closure of one or more establishments; and publication or dissemination of the decision at the expense of the convicted person).

In summary, although Belgium has a wide range of sanctions, these are neither specifically tailored to nor applied in line with TF risks. Some measures may be disproportionate to the size of the entities, while others, such as ex officio deregistration or judicial dissolution, do not have a purpose directly linked to combating TF.

Criterion 8.5 –

(a) In Belgium, there is no formal organisational framework for cooperation, coordination and exchanges of information between all authorities holding relevant information on NPOs, as required by C.8.5(a). This lack of a systemic coordination mechanism is exacerbated by the difficulty in obtaining a clear and up-to-date map of NPOs at risk in the country (see C.8.1), which limits the ability to have a coherent overview of the sector and to act in a coordinated manner.

However, mechanisms for cooperation and exchanging information on certain NPOs do exist, particularly between authorities involved in countering terrorism and its financing. These include exchanges between the Belgian Financial Intelligence Unit (CTIF), Central Unit for Threat Analysis (OCAM), State Security Service (VSSE), the police and the federal public prosecutor's office, which are facilitated by coordination platforms such as MONITOR, Joint Intelligence Centres /Joint Decision Centres, which ensure strategic and operational consultation between agencies (see IO.9). These channels facilitate regular and structured flows of information, for both preventive and repressive purposes, and may incidentally cover certain aspects relating to NPOs.

For places of worship, a formal framework for cooperation has been established between the different levels of authority, with a structured exchange of information under the cooperation agreement of 2 July 2008. SPF Justice collaborates with the VSSE, OCAM and CTIF during the recognition process. There is also collaboration with VSSE and OCAM concerning the *Banque de données communes* (BDC) (see IO.9). OCAM also collaborates with various national and international partners, including the police and intelligence services.

These sectoral examples show that targeted coordination can exist, although does not extend to all NPOs potentially at risk of FT.

(b) The Belgian legal and judicial framework enables the prosecution of terrorist financing cases, including when an NPO is involved. The common law investigative measures provided for in the Criminal Code fully apply to NPOs. The competent authorities have the necessary legal tools and operational capabilities to investigate NPOs suspected of being exploited for TF purposes, infiltrated by terrorist organisations or of actively supporting terrorist activities.

(c) As is the case for any legal person, access to relevant information relating to the administration and management of a particular NPO (including financial and business information) may be obtained as part of an investigation (see R.31). This includes any data held by an authority exercising control, registration or oversight over the NPO.

(d) Emergency procedures are provided for in COL 16/2024 governing the operation of inter-institutional platforms (JIC/JDC). If a TF risk is detected, an alert may be issued by the CTIF, the police (federal or local) or the intelligence services. The JIC/JDC process enables rapid coordination between authorities in the event of an emergency, especially to prevent the disappearance of funds (see IO.9).

Criterion 8.6 – International cooperation mechanisms have been put in place to respond to requests for information concerning NPOs suspected of financing terrorism. Mechanisms and procedures (other than mutual legal assistance) for international cooperation (particularly between FIUs) are provided for in the AML Law (Articles 122 to 131). However, Belgium has not designated any points of contact or defined appropriate procedures for responding to international requests for information (notably between non-counterpart authorities) concerning any NPO suspected of financing terrorism or supporting it by any other means.

> *Weighting and conclusion* – The authorities have not carried out a sufficiently precise identification of which subset of organisations meets the FATF definition of at-risk NPOs. As a result, the measures do not appear to be sufficiently targeted or specific to NPOs identified as being at risk of TF. **Belgium is partially compliant with R.8.**

Recommendation 9 – Financial institution secrecy laws[277]

Belgium was deemed compliant with R.9 in the 2015 MER.

Criterion 9.1 – There is no "banking secrecy" per se, but rather a contractual duty of discretion between the customer and the financial institution. This duty no longer applies where information must be transmitted to the judicial (see C.31.1.) and fiscal authorities, and to other organisations such as the monetary authorities, the prudential supervisory authorities and the CTIF, within the framework of their mission. Lastly, the privacy protection provided by law is waived when personal data needs to be processed in compliance with an obligation incumbent on the data controller or pursuant to legal or regulatory provisions, which is the case when information is required in AML/CFT matters (e.g. Law of 30 July 2018).

> *Weighting and conclusion* – **Belgium is compliant with R.9.**

Recommendation 10 – Customer due diligence

Belgium was rated largely compliant in the 2015 MER. Some shortcomings had been noted in the determination of beneficial owners, notably if the senior managing official was not designated as the beneficial owner where no natural person could be identified. The Follow-Up Report re-examined R.10 and reassessed it as compliant.

Criterion 10.1 – Belgian legislation prohibits the opening of anonymous accounts or accounts in obviously fictitious names(Art. 20 of the AML Law).

[277] Mutual Evaluation Report for Belgium (2015)

Application of customer due diligence

Criterion 10.2 – The due diligence obligation incumbent on financial institutions is based on legislative provisions (Art. 21 of the AML Law). It applies in the situations set out in R.10, with a threshold of EUR 10,000 for occasional transactions.

Criterion 10.3 – For customers who are natural persons and those who are legal persons, the documentary evidence required for identification and verification of identity are specified in the regulations. In general, official documents are required (Art. 19, 21, 26 and 27 AML Law; art. 10. et seq. BNB AML Regulation; Art. 12 et seq. FSMA AML Regulation).

Criterion 10.4 – The AML/CFT law requires the identification and verification of the customers' representatives, i.e. persons acting in any capacity whatsoever for them and on their behalf, using documentary evidence (Art. 7 §2). Financial institutions must also examine the powers of representation of persons acting on the customers' behalf and verify such powers with supporting documents of which they take copies (Art. 22 AML Law)

Criterion 10.5 – The AML/CFT law requires financial institutions to identify the beneficial ownership of the customer, and to take adequate risk-based measures to verify their identity. (Art. 23 of the AML Law). The definition of beneficial owner refers to the identification of a natural person (Art. 4, para.1, 27° AML Law).

To determine the identity of the beneficial owner, in addition to the information provided by the customer, the financial institution may refer to the company's register of units/shares, to which the customer must provide access, or to the UBO register (C.24.6.). Such sources are not available for customers which are legal arrangements. Financial institutions must define adequate risk-based measures in their internal procedures to verify the identity of beneficial owners (Art. 12 BNB AML Regulation; Art. 10 FSMA AML Regulation). If the beneficial owners' identity cannot be verified by means of a conclusive document, the financial institutions' internal procedures must specify the other documents or information sources that they rely on and use for the verification, such as indirect access to the National Register, which enables the verification of the beneficial owner's identity, without concerning the prior requirement to determine its existence and identity. Where the measures stipulated in the internal procedures are implemented but do not enable the verification of a customer's beneficial owners' identity, the institution should keep written records of the measures effectively taken, so that it can subsequently prove that they were adequate and risk based.

Criterion 10.6 – Customer identification must also cover the purpose and intended nature of the business relationship (Art. 19 and Art. 34, §1 of the AML Law). Financial institutions should therefore obtain information about the customer's intentions as regards the type of business relationship it wishes to establish and the kind of transactions it wishes to perform within the framework of that relationship, as well as any useful and relevant information revealing the ultimate purpose of this relationship from the customer's standpoint.

Criterion 10.7 –

(a) Financial institutions must exercise ongoing due diligence with regard to the business relationship and scrutinise the transactions undertaken in addition to the source of funds, where necessary *(Art. 35 of the AML Law)*. In addition, financial institutions must pay particular attention to any transaction they regard as likely to be connected with ML/TF ("unusual transactions"4) .

(b) Ongoing due diligence is also required in respect of the business relationship by verifying and, where necessary, updating customer identification data and information in the financial institutions' possession, where they are informed that such data is no longer up to date, Art. 35, § 1, 2° of the AML Law. This obligation also applies in respect of information concerning customers' beneficial ownership. In the case of companies, legal persons and arrangements, beneficial-ownership-related information is updated at the financial institution's request (Art. 8 §3). Specific due diligence measures are required for legal persons and legal arrangements.

Specific CDD measures required for legal persons and legal arrangements

Criterion 10.8 – There is no explicit requirement for financial institutions to understand the nature of the customer's business or to be aware of its control and ownership structure in the case of legal persons or arrangements. However, this information is one of the elements required to implement the customer acceptance policy and ongoing due diligence (), and identify the beneficial owners (Article 23, $ 1 of the AML Law).

Criterion 10.9 – The identification and verification of the identity of legal persons and legal arrangements concern the required elements (Art. 21 and 26 of the AML Law, including the identification and verification of the identity of the person(s) acting in any capacity whatsoever in the name of and on behalf of the legal person or legal arrangement (Art. 22 of the AML Law, see C.10.4).

Criterion 10.10 – The AML/CFT Law defines the beneficial owner of companies as including both a) persons which directly or indirectly control more than 25% of the shares or voting rights, and b) persons which otherwise exercise control over the management of the company, either where they exercise control without owning more than 25% of the voting rights, or where they are appointed to its administrative body. The provisions of the law stipulate that when the financial institution has exhausted all possible means and there are no grounds for suspicion, it must identify the company's senior managing official as the beneficial owner when no natural person can be identified. Accordingly, when the control criterion cannot be applied, the new legislative provisions enable the senior managing official of a company to be designated as the beneficial owner (Art. 4, 27° of the AML Law).

Criterion 10.11 – In the definition of the beneficial owner of legal persons other than companies, the AML Law includes persons who are beneficiaries of at least 25% of the assets of the legal person or legal arrangement, persons in whose interest the legal person was principally formed or acts, and persons who exercise control over at least 25% of the assets of the legal person or legal arrangement (Art. 4, 27° AML Law). Under the law, the relevant legal entities and arrangements are required to disclose the identity of their beneficial owners to the financial institutions of which they are customers. Financial institutions are required to test this information for credibility and relevance (Art. 26 and 29 of the AML Law), see C. 24.6. Due diligence for beneficiaries of life insurance policies.

CDD for Beneficiaries of Life Insurance Policies

Criterion 10.12 – There is no specific provision in the law or regulations concerning the identification of the beneficiary of a life insurance policy. However, the general framework allows for due diligence to be exercised in respect of the beneficiary of such a policy. The identification and verification of the identity of the beneficial owner to whom the benefit will be paid under the life insurance policy may be carried out at the latest when payment of the indemnity is claimed under the policy, and prior to payment thereof. This provision applies to the beneficiary of the policy, considered as one of the beneficial owners () (Art. 26, § 1, para. 2, AML Law).

Criterion 10.13 – There is no specific provision requiring financial institutions to consider the beneficiary of a life-insurance policy as a relevant risk factor when determining whether enhanced due diligence should be applied. However, financial institutions have a general duty to implement enhanced due diligence in all situations that may pose a high risk (Art. 19 of the AML Law). Where the characteristics of the beneficiary of the life-insurance policy (pursuant to the criteria of Article 19, § 2 of the AML Law) suggest that the business relationship involves higher risks, enhanced due diligence, including identification of the beneficial owner, is required, see 10.12.

Time of verification

Criterion 10.14 – Article 30 of the AML Law requires financial institutions not to enter into any business relationship or perform any occasional transactions until they have complied with their due diligence obligations in respect of potential customers and their beneficial owners.

The general exemption from this requirement (Art. 31 of the AML Law) provides that the circumstances warranting the postponement of the verification must not entail any interruption of the activities between the financial institution and the customer. In this case, the identity verification must be carried out as soon as possible after the first contact with the customer, and enhanced due diligence measures must be applied to ensure that ML/TF risks are effectively controlled. *(Art. 37 of the AML Law).*

Criterion 10.15 – Financial institutions wishing to use the option to postpone the verification of customers' identity must first define the specific circumstances in their internal procedures and then specify the precise arrangements in their customer acceptance procedure, under the supervision and responsibility of the AML/CFT prevention officer (Art. 30 and 31 of the AML Law). Enhanced due diligence measures must be applied until the identities of all the persons involved have been verified (see C.10.14).

Criterion 10.16 – The Law of 18 January 2010 provides for transitory provisions to enable the new provisions to be implemented by financial institutions in respect of existing customers (Art. 44). The five-year period for financial institutions to record information relating to customers' place and date of birth (Art. 44 para. 1) seems long, even in the absence of high risk, and insofar the financial institutions were already aware of this data. For the identification of beneficial owners, the times allowed for compliance have been set on a risk-sensitive basis, with a deadline of less than two years set for high-risk cases (Art. 44 para. 2).

Risk-based approach

Criterion 10.17 – The law requires financial institutions to apply enhanced due diligence in respect of their customers on a risk-sensitive basis, in situations which, by nature, present a high ML/TF risk (Art. 26, §4 and Art. 27, §4 of the AML Law).

For certain specific situations (PEPs, correspondent banking), minimum enhanced measures are stipulated, including obtaining authorisation from an appropriate management level to establish the business relationship or to carry out a transaction. (Art. 37 et seq. of the AML Law).

The provisions setting out the customer acceptance policy also require each financial institution to define a scale of risks based on which customers are allocated to different categories with different levels of requirements (Art. 4 of the BNB AML Regulation; Art. 4 of the FSMA AML Regulation), which takes full account of situations of increased risk.

Criterion 10.18 – The Belgian authorities state that less stringent due diligence measures apply to the categories of customers referred to in Article 19, § 1, para. 2 of the AML Law. This provision should be read in conjunction with article 26, § 3, 27, § 3, and 34, § 1 of the AML Law, which requires the person or institution to obtain sufficient information to be satisfied that the conditions laid down in §1 are met. The combination of these provisions inevitably requires identification and verification of the customer's identity, albeit simplified. However, these situations are based on a presumption of relatively low level of risk, without conducting any national or supranational analysis of the risks associated with each category of customer, which would establish the lowest ML/TF risk. In any event, the provisions of Article 19, § 2, para. 2 of the AML Law cannot be applied when ML/TF suspicions arise (C.1.12).

Inability to meet customer due diligence obligations

Criterion 10.19 – Where financial institutions are unable to fulfil their obligations to identify the customer or beneficial owner, they may not enter into or continue a business relationship, or carry out any transaction with the customer. In these cases, financial institutions must determine whether it is necessary to inform the CTIF (Art. 33 of the AML Law).

Criterion 10.20 – There is no provision in Belgian AML/CFT legislation authorising financial institutions to dispense with the identification of customers when they suspect that a transaction relates to ML/TF and have reason to believe that they would alert the customer by exercising their due diligence obligation.

> *Weighting and conclusion* – **Belgium is compliant with R.10.**

Recommendation 11 – Record-keeping

R.11 has been reassessed because Belgium has introduced legislative changes, in the AML Law of 2017, which revises the record-keeping obligations. Belgium was rated compliant with Recommendation 11 in the 2015 MER.

Criterion 11.1 – The AML Law's record-keeping provisions mirror those of the 1993 Law (deemed compliant in the 2015 MER), with the retention period increased from 5 years to 10 years. Financial institutions (FIs) are required to keep all the documents needed to identify and precisely reconstitute the domestic and international transactions carried out for a period of 10 years after the end of the business relationship with the customer or of an occasional transaction (Art. 60 AML Law).

Criterion 11.2 – The record-keeping system includes documents obtained as part of customer due diligence measures (including agents and beneficial owners), account books and business correspondence (Article 60, para. 1, 2°, AML Law).

Criterion 11.3 –Financial institutions are required to keep the data obtained in the framework of due diligence measures in order to enable them to accurately reconstruct the transactions carried out (Art. 60, 2° AML Law) and, where applicable, to respond to requests for information from the competent authorities within the scope of their respective powers (Art. 63, AML Law).

Criterion 11.4 – FIs must implement systems that enable them to respond fully, and via secure channels guaranteeing total confidentiality, to requests for information from the CTIF or the judicial and supervisory authorities (Art. 63, AML Law). Although the explanatory memorandum to the AML Law mentions making the information available "without delay" (page 187), this indication is not binding and does not appear in the body of the law. There are no provisions in any legislation on the deadlines by which FIs must provide the competent authorities with the information obtained under the due diligence obligations.

> *Weighting and conclusion* – The legislation does not specify any specific deadlines for the provision of information by FIs (C.11.4). **Belgium is largely compliant with R.11.**

Recommendation 12 – Politically exposed persons (PEPs) [278]

Belgium was rated partially compliant with R.12 in the 2015 MER. R.12 was re-rated compliant in the 2018 Follow-Up Report.

Criterion 12.1 – When PEPs have ceased to exercise a significant public function, the obliged entities shall consider, for at least twelve months, the risk that these persons continue to pose and shall apply appropriate measures, based on the assessment of this risk, until these persons no longer pose risks specific to PEPs (Art. 41 §3, AML Law). Consequently, there is a minimum period of one year during which obliged entities must

[278] Follow-Up Report for Belgium (2018)

apply measures adapted to the risk, specifying that additional due diligence measures must be applied beyond this period if the person poses a risk specific to PEPs.

Criterion 12.2 – The AML Law defines PEPs in accordance with FATF standards, including domestic and foreign PEPs and persons who hold or have held important posts within or on behalf of an international organisation (Art. 4, 28°, h, AML Law).

Criterion 12.3 – The definitions of "family member" and "persons known to be closely associated" are broad enough to comply with R.12 (Art. 4, 29° and 4,30°, AML Law).

Criterion 12.4 – There are provisions for identifying and verifying the identity of the beneficiaries of life insurance policies and their beneficial owners. In the case of a PEP, in addition to customer due diligence measures, obliged entities must inform a member of senior management prior to the payment of insurance benefits and carry out enhanced monitoring of the business relationship on an ongoing basis (Art. 41§2, AML Law).

> *Weighting and conclusion* – **Belgium is compliant with R.12.**

Recommendation 13 – Correspondent banking[279]

Belgium was rated partially compliant with R.13 in the 2015 MER. The partially compliant rating was maintained in the 2018 Follow-Up Report when R.13 was reassessed. The remaining shortcoming concerns the absence of an explicit obligation to apply the measures required by R.13 to cross-border correspondent banking relationships within the EEA.

Criterion 13.1 – The AML Law enacted on 18 September 2017 abolished the concept of equivalent third countries. For cross-border correspondent banking relationships with an institution in a third country (i.e. an institution outside the EEA), Article 40 provides for additional measures to be taken in accordance with R.13. These specific due diligence measures do not cover relations with establishments in the EEA.

Criterion 13.2 – Where a correspondent banking relationship involves the maintenance of payable-through accounts, the AML Law requires Belgian financial institutions to be satisfied, firstly, that the foreign institution has verified the identity and taken the required due diligence measures in respect of customers having direct access to the accounts opened with the Belgian institution, and secondly, that the foreign institution is able to immediately provide, on request from the Belgian institution, the relevant identification data of these customers (Art. 40 §1. para. 1, 5°, AML Law).

Criterion 13.3 – The law provides that financial institutions may not enter into or continue a correspondent banking relationship with a shell bank, and must take appropriate measures to ensure that they do not enter into or continue a correspondent banking relationship with an institution that is known to permit its accounts to be used by a shell bank (Art. 40 §2 and 4 37° for the definition of a shell banking company).

> *Weighting and conclusion* – Although the law provides for a general obligation to apply enhanced due diligence measures in high-risk cases, there is no explicit obligation to apply the measures required by R.13 for cross-border correspondent banking relationships within the EEA. **The level of compliance with R.13 therefore remains "partially compliant".**

[279] Follow-up Report for Belgium (2018)

Recommendation 14 – Money or value transfer services[280]

Belgium was rated largely compliant with R.14 in the 2015 MER. The applicable framework was reassessed at the time of the 2018 Follow-Up Report but the rating was maintained as largely compliant because the proportionality and deterrent nature of the penalties applicable to persons providing money or value transfer services without being licensed or registered could not be established. R. 14 is subject to a new assessment to take into account the entry into force of the Law of 11 March 2018 on payment institutions and electronic money institutions, which occurred after the 2018 follow-up report.

Criterion 14.1 – Payment services are listed in Annex I of the Law of 11 March 2018 on Payment Institutions and Electronic Money Institutions, and include money transfers. The National Bank of Belgium (BNB), the European Central Bank, the Belgian federal, regional, community and local authorities when they are not acting as public authorities, as well as Bpost, are among the institutions authorised by law to provide payment services (Art. 5), without having to obtain prior authorisation due to their status. The other financial institutions offering money transfer services covered by Annex I of the law – credit institutions, electronic money institutions and payment institutions – are subject to a requirement to obtain authorisation in their respective capacities from the BNB (R.26). Institutions which are "exempt" from certain requirements, pursuant to Directives 2007/64 and 2009/110, based on their size or volume of business, may not, however, be exempt from the requirements under the AML/CFT Law (provided for in Art. 21, 87§4, 176 and 203§4 of the Law of 11 March 2018). Credit and electronic money institutions governed by the law of another EEA Member State are authorised, pursuant to the principle of mutual recognition, to provide these services in Belgium, provided that this is permitted by the authorisation granted in their home Member State (Art. 5 1° and 2°). The BNB is notified by the competent authority of the home Member State when these undertakings intend to carry out activities in Belgium (Art. 312 and 313 of the Law 25 April 2014, and 120 et seq. and 218 et seq. of the Law of 11 March 2018). The terms and conditions for the provision of similar services by branches of institutions governed by the law of a third country that is not a member of the EEA have not been defined by Royal Decree (Art. 144) and they may therefore no longer provide payment services in Belgium.

Criteria 14.2 – The AML Law provides for a regime of sanctions applicable in the event of infringements of Directive (EU) 2015/849. This regime is linked to the legislative provisions relating to the FSMA (Law of 2 August 2002) and to the provisions of the Law of 11 March 2018. Under this regime, the FSMA has the power to investigate and sanction persons who provide money or value transfer services without authorisation or registration. The sanctions regime has remained unchanged since 2018; it is based on the 2002 and 2017 laws and predefined legal criteria (Art. 72, §3, 2002 Law).

Criteria 14.3 – Credit institutions, electronic money institutions that provide payment services, payment institutions under Belgian law and European institutions that offer such services in Belgium through a branch or agents are subject to the Belgian AML/CFT regime and are under the supervisory authority of the BNB (Art. 5 §1 and 15 AML law). Bpost acts as an agent for a European payment institution for its fund transfer operations. This payment institution is therefore subject to AML/CFT requirements in the context of the money transfer activities it carries out in Belgium through Bpost. Bpost acts as a central contact point for these specific transfer activities, for which it is placed under the supervision of SPF Finance (R.26). European payment institutions offering services in Belgium under the freedom to provide services are subject to supervision by the authority in their home country.

[280] Recommendation 14 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its 2018 Follow-Up Report.

Criterion 14.4 – Belgian payment service providers which use agents in Belgium are required to register them with the BNB (Art. 71-72 of the Law of 11 March 2018). Service providers authorised by another EU/EEA Member State who provide payment services in Belgium through agents are subject to the same obligations (Art. 127 of the Law of 11 March 2018).

Criterion 14.5 – Payment service providers which use agents established in Belgium or abroad are required to provide the BNB in advance with a description of the internal control mechanisms which the agent has put in place in order to comply with the obligations laid down by the European Regulation on transfers of funds and by the AML Law (Art. 71, para. 2, 4° of the Law of 11 March 2018), and carry out an audit at least once a year (Art. 73 of the Law of 11 March 2018). Service providers must include their agents in their AML/CFT programmes and ensure that these agents comply therewith (Art. 8, § 2, 2°, b) and 3°, Art. 10, 11, 36, 49, para. 2, 55, 55, 59 and 90 of the AML Law and Art. 19 and 20 of the BNB AML/CFT Regulation).

Weighting and conclusion – **Belgium is compliant with R.14**.

Recommendation 15 – New technologies[281]

Belgium was rated largely compliant in the 2015 MER. The requirements of R.15 were significantly amended by the FATF in 2018.

New technologies

Criterion 15.1 – Belgium is subject to the requirement to identify and assess the ML/TF risks to which the country is exposed (Art. 68 AML Law), which requires consideration of potentially higher or lower risk factors when assessing the risks associated with specific products, services, transactions or distribution channels (Art. 69 §2 AML Law). Financial institutions (FIs) are subject to an identical obligation (Art. 16 AML Law).

Concerning the obligation applicable to Belgium, Art. 69 §2 of the AML Law refers to the risk factors listed in Annexes 2 and 3 of the AML Law. Annex 3 Art. 1, 2° e) of the AML Law explicitly refers to the new products and new commercial practices covered by C. 15.1. Annex 2 is more restrictive in its approach (Art. 1, 2°, e)). Furthermore, these Annexes only refer to Article 16 of the AML Law for their application, which refers to assessments carried out by FIs and not by the country. It would therefore appear necessary to clarify the scope of Annexes 2 and 3 Art. 1 of the AML Law.

Criterion 15.2 – **(a)** and **(b)** The general obligations of the AML Law and the applicable BNB and FSMA Regulations[282] regarding risk assessment and measures taken for risk management and mitigation, and the application by Belgium of the European Banking Authority (EBA) guidelines on risk factors, create an obligation for FIs to assess risks before launching or using new products, practices and technologies and to take mitigating measures (Art. 8, 16 and 19 §2 of the AML Law; guideline 1.7 d) of the EBA Guidelines on Risk Factors with which Belgium has declared its compliance pursuant to Art. 16 point 3 of Regulation EU 1093/2010).

[281] R.15 has been reassessed because of the changes made to the FATF standards, for which Belgium has not previously been assessed.

[282] The BNB and FSMA Regulations meet the conditions of *Enforceable Means* within the meaning of the note on the legal basis of the obligations of FIs and DNFBPs and VASPs, Methodology p. 201, seethe introduction.

Virtual assets and virtual asset providers

Criterion 15.3 –

(a) Belgium is subject to the requirement to identify and assess the ML/TF risks to which the country is exposed, also taking account of the supranational risk assessments carried out by the European Commission (Art. 68 and 69 §1 AML Law). The 2023 ML and TF NRAs (see c. 1.1) include some virtual asset (VA)-related analysis, covering only virtual asset service providers (VASPs)' activities currently covered by the AML/CFT regime (see below). At EU level, the European Commission conducts and publishes an assessment of the risks of ML and TF affecting the internal market and relating to cross-border activities in line with the requirements of the EU Directive 2015/849 as amended by EU Directive 2018/843 (Art. 6) that also identifies and assesses the risks emerging from VA and the activities and operations from VASPs. The EU level risk assessment shall be updated by a report at least every two years.

The application in Belgium of the new European rules governing VASPs (amendment of Directive 2015/849 making all types of VASP covered by R.15 and governed by Regulation 2023/1114 on markets in crypto-assets ("MiCA Regulation") entities subject to European AML/CFT rules) is not yet effective. The measures transposing the provisions of Directive 2015/849 as amended by Regulation 2023/1113 on information accompanying transfers of funds and certain crypto-assets ("Transfer of Funds Regulation", TFR), as well as the Belgian national measures determining the framework for implementing the MiCA Regulation (designation of the authorities responsible for issuing licenses and exercising the AML/CFT supervision of all types of VASP), due by 30 December 2024, had not yet been adopted at the end of the on-site visit (14 February 2025).

In the absence of these measures, the implementation of the European framework in force in Belgium is incomplete, i.e. its implementation only covers the existing Belgian provisions subjecting two categories of VASPs to compliance with the AML Law: VASPs carrying out activities involving exchanges between virtual assets and fiat currencies, and the custody and/or administration of virtual assets or instruments enabling the control of virtual assets (Art. 4, 35°/2 and 3 and Art. 5, §1er 14/1 and 2 of the AML Law), activities referred to in (i) and (iv) of the FATF definition of VASPs). The other categories of VASP referred to by the FATF are not currently entities subject to AML/CFT measures in Belgium. In addition, in the absence of designation by Belgium of the competent authority for the licensing of VASPs in accordance with the requirements of the European framework in force, no VASP, irrespective of the activities it carries out, can be legally established in Belgium.[283] These shortcomings affect compliance with all the requirements of the following criteria of R.15.

There is no obligation to identify and assess PF risks.

(b) (i) On the basis of the national risk assessment, the Belgian authorities identify the measures to be taken in fields requiring enhanced due diligence and formulate recommendations to improve the allocation and prioritisation of resources (Art. 8, 19, 70 1° and 3° of the AML Law), which has been initiated to a certain extent with the AML action plan (see c. 2.1). **(ii)** There is no PF-related obligation.

(c) All entities subject to the requirements of the AML Law, including VASPs, are required to take measures to identify and assess their ML and TF risks (Art. 16, AML Law). They must also take appropriate measures to manage and mitigate these risks (Art. 8 and 19 §2, AML Law). There is no PF-related obligation.

Criteria 15.4 to 15.8 and criterion 15.11 –There were no applicable arrangements for the licensing or registration of all types of VASPs in Belgium and the designation of an AML/CFT supervisory authority at the end of the on-site visit (14 February 2025), see C.15.3. (a). For VASPs already subject to the provisions of the AML Law, the provision of the services concerned requires registration in the relevant register (Art. 5, § 1, para. 3 of the AML Law and Art. 4 §1 of the Royal Decree (RD) of 8 February 2022). This requirement has

[283] At the time of the on-site visit, no VASP was registered or authorised in Belgium (see Chap. 1, section 1.2.1 and IO 3).

been rendered inapplicable since the MiCA Regulation entered into force on 30 December 2024, imposing a licensing procedure for these VASPs (Articles 59 to 65). Consequently, at the end of the onsite visit, no VASP could be licensed nor legally provide virtual asset services from Belgium.

Criterion 15.9 – VASPs subject to Belgian AML/CFT requirements (see C. 15.3 a)) are subject to the preventive measures of Recommendations 10 to 21, under the conditions set out in the AML Law.

(a) Occasional transactions in the form of electronic transfers exceeding EUR 1,000 require the application of customer due diligence measures under the conditions provided for by R.10 (Art. 21 §1, 2° b) of the AML Law).

(b) (i) EU Regulation 2023/1113 repeals and replaces EU Regulation 2015/847 formerly regulating the transfer of funds and extends the scope to cover both transfer of funds and transfer of virtual assets. Art. 14 (1) of EU Regulation 2023/1113 requires the originating crypto asset service provider to obtain and hold originator information (Art. 14 (1), (2) and (3)) and to submit it to the beneficiary service provider immediately (in advance or simultaneously) and securely (Art. 14 (4)). Before transferring crypto-assets, the service provider shall verify the accuracy (Art. 14 (6). In accordance with Art. 24 of EU Regulation 2023/1113, information has to be provided to competent authorities in the Member State in which they are established. The originating crypto asset service provider submits beneficiary information to the beneficiary's service provider in line with Art. 14 (2) of Regulation 2023/1113 and holds it on record according to Art. 26 (1) Regulation 2023/1113.

The distributed ledger address (DLT) information is required for both the originator and the beneficiary. If the transfer does not occur on the DLT, the Regulation requires the crypto-asset account number instead (EU Regulation 2023/1113, Art.14 (1) (b) and (2) (b)).

EU Regulation 2023/1113 imposes additional requirements to be implemented in the case of transfers being made to self-hosted addresses (where no crypto asset service provider is involved on the originator or beneficiary side), such as individual identification of transfers and ensuring that the address is controlled by the originator/beneficiary.

EU Regulation 2023/1113 does not make a distinction between crypto-asset transfers within and outside the EU, treating all crypto-asset transfers as cross-border.

(ii) Art. 16 of EU Regulation 2023/1113 requires the crypto asset service provider of the beneficiary to implement effective procedures, which may include post-event or real-time monitoring, to identify transfers that lack required originator or beneficiary information and to verify accuracy of the beneficiary information (EU Regulation 2023/1113, Art. 16 (1) and (3)). Service providers are obliged to make information available to competent authorities on request according to Art. 24 of EU Regulation 2023/1113

(iii) EU Regulation 2023/1113 covers the requirements of Recommendation 16 and applies them to virtual asset transfers, especially on monitoring and risk-based procedures (Art. 14 (8) and Art. 16 (1)) as well as freezing action and prohibiting transactions with designated persons and entities (Art. 23).

(iv) Financial institutions are covered by the scope of relevant provision of EU Regulation 2023/1113 through the broad definition of crypto asset service provider in Art. 3 (1) 15 of that Regulation with reference to Art. 3 (1) (15) EU Regulation 2023/1114, including credit institutions that provide crypto asset services in accordance with Art. 59, 60 of EU Regulation 2023/1114.

Criterion 15.10 – The mechanisms for communicating designations and the reporting and monitoring obligations set out in criteria 6.5(d) and (e), 6.6(g), 7.2(d) and (e), 7.3 and 7.4(d) apply to VASPs with the limitations identified in R.6 and 7, and those related to the limited scope of VASPs in Belgium.

> *Weighting and conclusion* – Belgium's failure to adopt the measures transposing the provisions of Directive 2015/849 as amended by the TFR, and the Belgian national measures determining the

framework for implementing the MICA Regulation, are major shortcomings given the ML/TF risk posed by these players, who could only operate illegally on the Belgian market due to the absence of a legal framework and designated competent authority, and the proven cases of increasing use of virtual assets in ML and TF schemes (see IO 1, 7, 8 and 9). **Belgium is non-compliant with R.15.**

Recommendation 16 – Wire transfers[284]

R.16 has been reassessed following changes to the European framework for electronic credit transfers in Belgium. Belgium was rated partially compliant during the 2015 MER, under Regulation (EC) No 1781/2006. These Regulations have since been replaced by Regulation (EU) 2015/847, which has remedied the shortcomings identified in the 2015 MER, notably by introducing requirements concerning information about the originator (hereinafter referred to as the payer) and the beneficiary, maintained with the transfer of funds. This enabled the rating to be upgraded to compliant in the 2018 Follow-Up Report. The new Regulation (EU) 2023/1113 (hereinafter, the TFR) includes the same requirements as Regulation (EU) 2015/847.

Originator's financial institutions

Criterion 16.1 – In accordance with EU Regulation 2023/1113, Art. 4, 6, FIs should ensure that all cross-border wire transfers exceeding EUR 1,000 are accompanied by:

(a) required and accurate payer (originator) information (name, account number or, in the absence of an account, unique transaction reference, and address, document number, customer ID, or date and place of birth), and

(b) required payee (beneficiary) information (name, account number or, in the absence of an account, unique transaction reference).

The EU requirements for cross-border transfers do not apply to transfers equalling USD/EUR 1,000, which constitutes a minor deviation from the corresponding Recommendation.

Criterion 16.2 – Where several cross-border wire transfers from the same originator are transmitted in a batch file to beneficiaries, the batch file should contain the information required per criterion 16.1, and each individual wire transfer should contain the account number or unique reference number (EU Regulation 2023/1113, Art. 4, 6(1)).

Criterion 16.3 – Cross-border wire transfers of EUR 1,000 or less should be accompanied by the names and account numbers of the originator and beneficiary or the unique transaction reference number (EU Regulation 2023/1113, Art. 6(2)).

Criterion 16.4 – For cross-border wire transfers not exceeding EUR 1,000, the originator's financial institution is not required to verify the accuracy of the information about the originator unless it suspects ML/TF or the funds are transferred in the form of cash or anonymous electronic money (EU Regulation 2023/1113, Art. 6(2)). The same applies to the beneficiary’s financial institution (EU Regulation 2023/1113, Art. 7(4)).

Criterion 16.5 – For wire transfers with all participants in the payment chain established within the EU, Art. 5 (2) EU Regulation 2023/1113 obliges the service provider of the payer, upon request, to make all information on the originator or beneficiary available to the beneficiary's financial institution. Based on the

[284] Recommendation 16 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its 2018 Follow-Up Report

availability of this information by other means, Art. 5 (1) EU Regulation provides for a derogation of the comprehensive information requirements in line with c16.5.

Criterion 16.6 – FIs should ensure that the account numbers of the originator and beneficiary or their unique transaction identifiers accompany the transfer (EU Regulation 2023/1113, Art. 5(1)) even in applying the derogation in line with c16.5. FIs are required, upon request, to make all necessary information available within three working days (EU Regulation 2023/1113, Art. 5(2)). They are also required to respond fully and without delay to requests issued by the authorities responsible for AML/CFT (EU Regulation2023/1113, Art. 24).

Criterion 16.7 – The originator's financial institution is required to maintain all information collected on the originator and beneficiaries for a period of five years (EU Regulation 2023/1113, Art. 26).

Criterion 16.8 – The originator's financial institution is not allowed to execute wire transfers if they do not comply with the requirements under Criteria 16.1 to 16.7 (EU Regulation 2023/1113, Art. 4(6)).

Intermediary financial institutions

Criterion 16.9 – FIs acting as intermediaries should ensure that all originator and beneficiary information accompanying cross-border wire transfers is retained with the transfer (EU Regulation 2023/1113, Art. 10).

Criterion 16.10 – Technical imitations cannot justify non-compliance with the requirements under Art. 10 EU Regulation 2023/1113 and no exemption from the requirements described under criterion 16.9 is permitted. The "Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under EU Regulation 2023/1113" issued by the European Banking Authority on 4 July 2024 reflect that systems have to be able to transmit, receive or convert all information (section 4.3.1., para 21, 22).

Criterion 16.11 – Intermediary FIs should implement effective procedures to identify cross-border wire transfers that lack the required originator or beneficiary information (EU Regulation 2023/1113, Art. 11, point 2(b)).

Criterion 16.12 – Intermediary FIs should have risk-based procedures in place to determine whether to execute, reject or suspend a wire transfer that does not include the required originator or beneficiary information, and to take appropriate follow-up action (EU Regulation 2023/1113, Art. 12).

Beneficiary financial institutions

Criterion 16.13 – FIs should implement effective procedures, which may include post-event or real-time monitoring, to identify cross-border wire transfers that lack required originator or beneficiary information (EU Regulation2023/1113, Art. 7 (2)).

Criterion 16.14 – For wire transfers exceeding EUR 1,000, the beneficiary's financial institution should verify the identity of the beneficiary (EU Regulation 2023/1113, Art. 7(3)) and should retain this information for a period of five years (EU Regulation 2023/1113, Art. 26).

For wire transfers equalling EUR 1,000, the beneficiary's financial institution is not required to verify the accuracy of the information unless it suspects ML/TF or the funds are transferred in the form of cash or anonymous electronic money (EU Regulation 2023/1113, Art. 7(4)), which constitutes a minor deviation from the corresponding Recommendation**.**

Criterion 16.15 – Beneficiary financial institutions should have risk-based procedures in place to determine whether to execute, reject or suspend a wire transfer that does not include the required originator or beneficiary information, and to take appropriate follow-up action (EU Regulation 2023/1113, Art. 8).

Money or value transfer service operators

Criterion 16.16 – EU Regulation 2023/1113 applies to payment service providers established in the EU or EEA that execute fund transfers, whether they operate directly or through their agents (EU Regulation 2023/1113, Art. 2(1)).

Criterion 16.17 –

(a) *Analysis of information from the originator and beneficiary:* Payee and intermediary payment service providers should take into account missing or incomplete information on the originator or beneficiary in order to assess whether a suspicious transaction report should be filed (EU Regulation 2023/1113, Art. 9 and 13).

(b) *Suspicious transaction report:* There is no explicit obligation requiring payment service providers to file a suspicious transaction report in all countries concerned by a suspicious wire transfer. However, payment service providers are obliged to report in the countries of the ordering and beneficiary sides (Regulation (EU) 2023/1113, Art. 9 and 13) of the transaction and service providers belonging to the same financial group are required to inform the members of the group of the existence and content of a suspicious transaction report relating to a common client (Art. 45 EU Directive 2015/849).

Implementation of targeted financial sanctions

Criterion 16.18 – FIs should implement freezing measures and comply with prohibitions from conducting certain transactions in accordance with EU regulations which give effect to UNSCR relating to AML/CFT (cf. R. 6 and 7). EU Regulation 2023/1113, Art. 23 requires payment service providers to have in place internal policies, procedures and controls, in alignment with the Guidelines adopted pursuant to Article 23(2) of the Regulation to ensure the implementation of EU and national restrictive measures.

> *Weighting and conclusion* – A minor shortcoming remains concerning the transmission of a suspicious transaction report to the FIU of the State involved in the transfer when suspicious transfers involve several countries. **Belgium is therefore largely compliant with R.16.**

Recommendation 17 – Reliance on third parties[285]

Belgium was rated partially compliant with R.17 in the 2015 MER. The main shortcomings stemmed from the existence of an exemption regime for third-party introducers from EEA countries or equivalent third countries. This made it impossible to verify the satisfactory application of AML/CFT measures applied by these institutions. It is also important to emphasise that the inclusion of countries on the list of equivalent third countries took account of risk-related factors without this analysis focusing on ML/TF risks. R.17 was reviewed in the 2018 Follow-up Report and the rating upgraded to largely compliant, with persistent failings related to the existence of an exemption regime for countries in the European Area that are not considered third countries under the ban on obliged entities using third party introducers established in high risk countries.

Criterion 17.1 – The 2017 AML Act sets out a framework for the use of third-party introducers by obliged entities. This framework incorporates the obligations set out in the previous scheme, but removes the equivalent third country concept. Obliged entities wishing to use a third-party introducer governed by the law of a third country must determine whether the legal and regulatory provisions and the supervision to

[285] Follow-Up Report for Belgium (2018)

which the third party is subject meet the equivalence conditions laid down. It is also stipulated that reporting entities may not use third-party introducers established in high-risk countries (Art. 43 § 2 of the AML Law). However, an exemption scheme remains in place for EEA countries that are not considered third countries.

Criterion17.2 – The third-party introducer may be based in Belgium, in another EEA member country or in an equivalent third country (Art. 43 para 1, AML Law). The use of the services of financial institutions located in EEA member countries is not based on information about the country's AML/CFT risks but reflects the presumption that all EEA members implement harmonised AML/CFT provisions pursuant to the third AML/CFT Directive. Inclusion on the list of equivalent third countries takes account of the compliance of local legislation with the main FATF Recommendations, and the level of risk linked to the degree of criminality to which the country in question is exposed and which constitutes threat of ML. Risk-related factors are therefore taken into account, without this analysis being targeted at ML/TF risks.

Criterion 17.3 – Belgium has not made use of the option to introduce specific measures in its framework to modify the manner in which a financial institution must meet its obligations when the third party introducer is part of the same financial group

Weighting and conclusion – **Belgium is largely compliant with R.17.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries[286]

R.18 has been reassessed following changes made to the AML Law by the Law of 20 July 2020. Belgium was rated partially compliant in the 2015 MER, and was then rated largely compliant in its 2018 Follow-Up Report. The remaining minor shortcomings concern the scope and extent of the information transmitted by branches and subsidiaries in the context of information sharing.

Criterion 18.1 – Financial institutions (FIs) must adopt AML/CFT policies, procedures and internal control measures appropriate to the size and nature of their business (Art. 8, § 1, 1°, AML Law). These measures must be proportionate to the ML/TF risks identified and regularly updated (Art. 16 and 17, AML Law). FIs are legally required to:

(a) designate persons responsible for the application of policies, procedures and internal control measures, and for proposing any measures necessary to ensure the compliance and effectiveness of the AML/CFT programme. These persons must be of good repute, possess appropriate AML/CFT expertise and have the necessary authority within the entity to perform their duties effectively, independently and autonomously (Art. 9, §2, para. 1 and 3). FIs must also designate a senior officer (within the management or administrative body) responsible for the overall implementation of and compliance with AML/CFT obligations (Art. 9, § 1). Depending on the size or nature of the institution, certain functions may be performed by the same person (Art. 9, §3).

(b) implement selection procedures to ensure that employees are recruited according to demanding criteria. In particular, they must check the good repute of their staff, agents or distributors when they are recruited or assigned, taking account of the risks associated with the tasks and duties to be performed, as well as the nature and size of the institution (Art. 8, §2, 2°, b). They shall ensure that the persons involved in implementing AML/CFT obligations have the necessary qualifications (Art. 9, §2, para. 2).

(c) provide training and awareness-raising programmes for staff (including agents and distributors) on the ML/TF risks to which the FI is exposed (Art. 8, §2, 3°). FIs must also provide for staff participation in special

[286] Recommendation 18 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its 2018 Follow-Up Report.

in-service training programmes. This training must be adapted to their duties and to the ML/TF risks identified (Art. 11, §2).

(d) establish an independent audit function for all reporting entities, responsible for testing internal control policies, procedures and measures (Art. 8, §2, 2°, a). This requirement takes account of the size and nature of the obliged entity. However, the degree of flexibility applied to "small" FIs is not clearly defined to ensure that a minimum audit mechanism is in place, including in small FIs.

Criterion 18.2 – Financial groups whose registered office is located in Belgium must establish an AML/CFT programme at group level (including subsidiaries and branches), whose policies and procedures apply to their constituent entities, without distinction between entities in Belgium, in the EU or in a third country (Art. 13, §1 of the AML Law transposing Article 45 of Directive (EU) 2015/849). However, this consistency requirement remains non-binding, with the explanatory memorandum to the Act simply specifying that this obligation for consistency within the group should extend to the functions of AMLCOs, the internal control levels, and the procedures for recruiting and training staff in AML/CFT matters.

For all entities subject to the AML Law, this programme must also include:

(a) AML/CFT prevention policies and procedures providing for the sharing of intra-group information necessary for AML/CFT vigilance, notably information relating to customers (including the identity of customers' authorised representatives and beneficial owners) and their transactions, taking account of data protection policies (Art. 13, §1, sub-para. 1 and 2).

(b) Article 13, §1, para. 1 and 2 establishes a general framework for sharing information for AML/CFT purposes, requiring entities in the same group, including branches and subsidiaries, to share all information necessary for the prevention of ML/TF. This framework also includes the possibility for Group compliance functions to pass on relevant information to branches and subsidiaries. This information includes the identity of customers, authorised representatives and beneficial owners, the purpose of business relationships, their transactions and, if necessary, an analysis of atypical transactions.

(c) Intra-group exchanges of information must be carried out in compliance with conditions guaranteeing confidentiality and the protection of personal data, including measures to prevent their disclosure (Art. 13, § 1, sub-para. 2).

Criterion 18.3 – FIs must ensure that their branches and majority-owned subsidiaries located abroad, whether inside or outside the EU, apply AML/CFT measures equivalent to those set forth in the Belgian AML Law [Art. 13, §1er]. Examples of such measures include data protection and information sharing policies within the group for AML/CFT purposes. FIs established in a third country must ensure that their local entities comply with the AML/CFT legislation in the host country, provided that this legislation is at least as strict as Belgian law. If this is not the case *(if local legislation does not permit the adequate implementation of requirements equivalent to those in Belgium*), the financial group must apply additional measures to manage ML/TF risks and notify the Belgian supervisory authorities without delay [Art. 13, §3, para. 3]. These additional measures are listed in Article 8 of the Delegated Regulation (EU) 2019/758, and may include: enhanced examinations, on-site inspections or independent audits, or limiting the financial products and services offered to those posing a low ML/TF risk.

Weighting and conclusion – There are shortcomings with regard to criteria 18.1(d) and 18.2. **Belgium is largely compliant with R.18.**

Recommendation 19 – Higher-risk countries[287]

Belgium was rated largely compliant with R.19 in the 2015 MER. Belgium lacked the instruments to decide, independently of an FATF decision, on countermeasures to be taken against countries posing higher risks. In the 2018 Follow-Up Report, Belgium's compliance with R.19 was reassessed as compliant.

Criterion 19.1 – Financial institutions implement enhanced due diligence measures, including the authorisation of a member of a senior management level (see C.10.17) for the establishment of business relationships or the conclusion of a transaction with customers involving a high-risk third country (Art. 4, 9° AML Law), including third countries posing a geographical risk defined as high by the FATF for which it recommends countermeasures or the exercise of enhanced due diligence (Art. 38 §1, AML Law). This enhanced due diligence continues for the duration of the business relationship, in application of the duty of ongoing due diligence (Art. 35 §2, AML Law).

Criterion 19.2 – Belgium has the capacity to apply countermeasures proportionate to the risks

(a) *where called upon to do so by the FATF* – Art. 38 §2 of the AML Law, applicable to transactions involving natural or legal persons or legal arrangements, such as trusts or *fiducies*, involving countries in respect of which the FATF is likely to call for such countermeasures, empowers the King to require obliged entities to apply one or more additional due diligence measures to persons and legal entities carrying out transactions involving high-risk third countries, and to apply measures in respect of such countries such as refusing to establish subsidiaries, branches or representative offices of reporting entities from the country concerned, or otherwise taking account of the fact that the obliged entity concerned originates from a country that lacks satisfactory arrangements for countering ML/TF. Such a Royal Decree has not been adopted.

(b) *independently of any appeal by the FATF*: the 2015 MER noted that Belgium lacked the necessary instruments to decide on countermeasures independently of an FATF decision. This shortcoming has since been rectified by Article 54 of the AML Law of 2017, which introduces measures enabling the King to take countermeasures by decree against countries or territories whose legislation is recognised as unsatisfactory or whose practices are considered to hinder the fight against ML/TF, regardless of any appeal from the FATF. These countermeasures are based on the national risk assessment or on the decisions of a competent consultation and coordination body at international or European level. The planned countermeasures consist in extending the reporting obligation for entities subject to the law. It is also stipulated that other countermeasures proportionate to the risks in the country concerned may be taken.

Criterion 19.3 – The CTIF systematically publishes a notice on its website for all persons and institutions subject to the AML/CFT law, informing them of the latest decisions taken by the FATF concerning countries with strategic AML/CFT deficiencies. It also provides reporting entities with information about concerns raised by weaknesses in the AML/CFT systems of other countries, which are not publicly identified by the FATF as posing a higher risk (e.g. Cyprus, Ukraine). The Treasury also has a website dedicated to higher-risk countries.

> ***Weighting and conclusion*** – By means of a Royal Decree, Belgium is now fully capable of applying countermeasures independently of a FATF decision. **Belgium is compliant with R.19**.

[287] 2015 MER and 2018 Follow-Up Report

Recommendation 20 – Reporting of suspicious transactions[288]

R.20 has been reassessed as the 2017 AML Law made changes relating to suspicious transaction reports. Belgium was rated compliant in the 2015 MER.

Criterion 20.1 – The AML Law (Art. 47 § 1 and 2) stipulates that all obliged entities are required to inform the CTIF of transactions for which they know, suspect or have reasonable grounds to suspect: 1) that the funds, irrespective of their amount, are linked to ML/TF; 2) that the transactions or attempted transactions are linked to ML/TF; or 3) that any fact of which they are aware is linked to ML/TF.

Belgian law requires that this report be submitted prior to the transaction, or "immediately" thereafter if this is not possible (Art. 51). However, the notion of "immediacy" cannot be fully assessed in the absence of any indication or specification of a timeframe, whether precise or indicative, to provide guidance.. Similarly, although the FSMA and BNB regulations require FIs to analyse atypical transactions "promptly" and diligently, the combination of these imprecise terms leaves significant room for interpretation by obliged entities. The absence of a clear or indicative time frame leads to a risk of variable or random interpretation by FIs, which can lead to unjustified delays in the transmission of reports to CTIF (see IO.3 and 4). This uncertainty may also make it more difficult for the supervisory authorities to monitor compliance with the obligation.

Criterion 20.2 – Attempted transactions must be reported (Art. 47 §1, 2°). The law makes no provision for any minimal amount in the reporting of a transaction or an attempted transaction.

> *Weighting and conclusion* – The lack of a clear definition of the notion of immediacy is a technical imprecision in the suspicious transaction reporting system. **Belgium is largely compliant with R.20**.

Recommendation 21 – Tipping-off and confidentiality[289]

Belgium was deemed compliant with R.21 in the 2015 MER. In November 2017, the FATF revised R.21 to clarify that the ban on disclosure of a suspicious transaction report or related information is not intended to prevent information sharing under R.18. The applicable framework in Belgium was reassessed in the 2018 Follow-Up Report and the compliant rating was maintained.

Criterion 21.1 – No civil, criminal or disciplinary action may be taken or professional sanction imposed against reporting entities or their managers, employees or representatives who have provided information to the CTIF in good faith. In addition, the AML Law provides for the protection of declarants against any threat, hostile act or intimidation (Art. 57, 2017 AML Law). Finally, when the CTIF issues a communication to the public prosecutor, the federal public prosecutor or its foreign counterparts, with a view to maintaining the anonymity of the authors of the reports the suspicious transaction reports (STRs) (and the supplementary STRs) are not legally part of the file sent to the public prosecutor's office.

Criterion 21.2 – In accordance with Article 55 §1 of the AML Law, reporting entities or their directors, employees or representatives may not, under any circumstances, inform the customer concerned or third parties that information has been transmitted to the CTIF in accordance with their STR duty or that an investigation in relation to ML/TF is in progress or may be opened. When a professional (notary, auditor, external accountant, external tax adviser, chartered accountant, chartered tax accountant or lawyer)

[288] R.20 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its mutual evaluation in 2015.

[289] Mutual Evaluation Report (2015) and Follow-up Report (2018)

endeavours to dissuade a client from taking part in an illegal activity, this does not amount to tipping off within the meaning of Article 55 § 1 (see C. 23.4).

Article 56 of the AML Law specifies that the ban on disclosing the fact that information is being, has been or will be transmitted to the FIU does not apply within the same financial group, thus satisfying the requirements of the revised Recommendation.

Weighting and conclusion – **Belgium is compliant with R.21**

Recommendation 22 – Designated non-financial businesses and professions (DNFBPs): customer due diligence[290]

R.22 has been reassessed to take account of the fact that company service providers are subject to the AML law. Belgium was rated largely compliant with the requirements of this Recommendation in the 2015 MER. The shortcomings identified concerned the failure to include company service providers in the AML/CFT framework. DNFBPs were also affected by the shortcomings identified under R.10, 11, 12, 15 and 17. The 2018 Follow-Up Report has since upgraded R.10 and 12 to compliant and R.17 to largely compliant.

Criterion 22.1 – The due diligence measures required by law are set out in the regulatory provisions applicable to each sector. DNFBPs are therefore required to comply with the customer due diligence obligations set out in R.10 in the following situations:

(a) *casinos* – when customers carry out gambling transactions amounting to EUR 2,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked (Art. 21, §1, 3° AML Law);

(b) *estate agents* – the obligation applies to all regulated activities carried out by estate agents, as referred to in Art. 5, §1, 30° of the AML Law, and in Art. 2, 5° and 7° of the Law of 11 February 2013 organising the estate agent's profession. This includes activities such as the intermediation of contracts for the sale, purchase, exchange, rental or transfer of property, property rights or business assets.

(c) *Dealers in metals and precious stones* – In Belgium, only diamond dealers are expressly subject to AML/CFT obligations [Art. 5, §1, 31°, AML Law]. Other dealers in metals (gold, platinum, silver) and precious stones are not subject to the obligation to implement preventive measures. This is because Belgium has introduced a ban on cash payments in excess of EUR 3,000 [Art. 67, §2, AML Law], a much lower threshold than the EUR 15,000 stipulated by the FATF Standards.

(d) *lawyers, notaries, other independent legal professionals and accountants* are subject to the AML Law (AML Law, Art.5 §1, 23°, company auditors; 24° and 25° chartered accountants 26° notaries; 28° lawyers). Lawyers must comply with the customer due diligence requirements set out in R.10 when preparing or carrying out transactions for their customer relating to any of the activities listed in C.22.1(d). Notaries, other independent legal professionals and accountants are subject to the AML Law for all their activities, including those listed in C.22.1(d), given that they are not carried out on a professional basis.

(e) *service providers to trusts and companies* (Art 5, §1, 29 AML Law) – In Belgium, there are only company service providers because Belgian law does not recognise trusts. This does not prevent the trustee function from being exercised in Belgium within the framework of a trust governed by foreign law (see R.25). These service providers must comply with the customer-related obligations set out in R10 only when preparing or carrying out transactions for a customer in connection with the provision of a registered office. The other four activities listed in C.22.1(e) are not covered by the AML Act.

[290] R.22 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its mutual evaluation in 2015.

Criterion 22.2 – Covered DNFBPs are required to comply with the same document retention requirements as FIs set out in R.11 with an identical limit noted in C.11.4 (Art. 63, AML Law).

Criterion 22.3 – Covered DNFBPs are required to comply with the same PEP requirements as FIs, in accordance with R.12 (Art. 4, 28° and 32°, Art. 41, §§1, 2 and 3, Art. 35, AML Law).

Criterion 22.4 – In the situations set out in criterion 22.1, DNFBPs are required to comply with the applicable obligations relating to new technologies set out in R.15 with an identical limitation observed in the analysis of R.15.

Criterion 22.5 – In the situations set out in criterion 22.1, DNFBPs must comply with the obligations relating to the use of third parties set out in R.17 (Art. 42 to 44, AML Law). The shortcomings identified in the analysis of R.17 apply to DNFBPs to the same extent.

The observations made in the analysis of C. 22.1 apply to the other requirements of R.22 to the same extent.

> *Weighting and conclusion* – The shortcomings raised under R.11 and R.15 also apply to this Recommendation. In addition, the shortcoming linked to the existence of an exemption regime for countries in the European Area that are not considered third countries under the ban on obliged entities using third party introducers established in high risk countries also applies to DNFBPs. **Belgium is largely compliant with R.22**.

Recommendation 23 – DNFBPS: other measures[291]

R.23 has been reassessed to take account of the fact that company service providers are subject to the AML law. Belgium was rated largely compliant with the requirements of this Recommendation in the 2015 MER. The shortcomings identified concerned the failure to include company service providers in the Belgian AML/CFT framework. DNFBPs were also affected by the limitations identified under R.18.

Criterion 23.1 – The suspicious transaction reporting obligations set out in R.20 apply to DNFBPs in the following circumstances:

(a) *Lawyers, notaries, other independent legal professionals and accountants* – lawyers must inform the President of the bar association to which they belong immediately. After verification, the President of the Bar forwards the information immediately to the CTIF (Art. 52, AML Law). However, since ruling No 114/2020 of 24 September 2020, the Constitutional Court has annulled the reporting obligation applicable to lawyers in the event of an unsuccessful attempted transaction. Notaries, other independent legal professionals and accountants are required to comply with the obligations to report suspicious transactions (Art. 47 and 51).

(b) *Dealers in precious metals or precious stones* – diamond dealers must comply with the suspicious transaction reporting obligations (Art. 47 and 51, AML Law).

(c) *Trust and company service providers* – company service providers are required to comply with suspicious transaction reporting obligations where they prepare or carry out transactions for a client in connection with the provision of a registered office (Art. 47 and 51 AML Law). As mentioned in the analysis of C.22.1(e), the other activities listed in C.22.1(e) are not covered by the AML system.

Criterion 23.2 – Covered DNFBPs are required to comply with the same requirements as FIs in respect of internal controls and foreign branches and subsidiaries, with an identical limit noted in the analysis of R.18.

Criterion 23.3 – Covered DNFBPs are required to comply with the same requirements as FIs with regard to higher-risk countries (Art. 38 and 54, AML Law).

[291] R.23 has been reassessed because of the changes made to the FATF standards and for which Belgium has not previously been assessed.

Criterion 23.4 – Covered DNFBPs are required to comply with the same disclosure and confidentiality requirements as FIs (Art. 55 and 90, AML Law).

> *Weighting and conclusion* – STR requirements are laid down by law, but lawyers are not required to declare attempted transactions. A number of other minor shortcomings have been noted, relating to compliance with the requirements of R.18. **Belgium is largely compliant with R.23**.

Recommendation 24 – Transparency and beneficial ownership of legal persons[292]

R.24 has been reassessed in the light of the amendments made by the FATF in March 2022, which significantly recast the requirements relating to the transparency of legal persons.

Belgium was rated largely compliant in the 2015 MER, notably because of the lack of a cross-sectorial assessment of ML/TF risks associated with the different categories of legal persons created in Belgium, shortcomings in the mechanisms put in place by Belgium to ensure that information on beneficial owners is accurate and kept up to date, the inadequacy of the mechanisms relating to shares registered in the name of nominees, the inability to conclude that the applicable sanctions are proportionate, and the absence of sanctions for legal persons (or their representatives) who submit false or misleading information on their beneficial owners to the professions subject to the obligations.

Criterion 24.1 – The entry into force of the new Belgian Companies and Associations Code (CSA) on 1st May 2019 has amended and unified the regulations for legal entities in Belgium. Three forms of legal entity may be created in Belgium: companies (Art. 1:1 and 1:5 CSA); associations (Art. 1:2 and 1:6 para.2 CSA); and foundations (Art. 1:3 and 1:7 CSA).

(a) The requirements of R.24 apply to all companies incorporated under Belgian law*:* ordinary partnerships, general partnerships (*sociétés simples, sociétés en nom collectif* – SNC), limited partnerships (*sociétés en commandite* – SComm), private limited companies (*sociétés à responsabilité limitée* – SRL), cooperative societies (*sociétés coopératives* – SC), and public limited companies (*sociétés anonymes* – SA), (Art 1:35, CSA). Companies listed on a regulated market are subject to specific financial information and publication obligations including the obligation to ensure sufficient transparency of beneficial owners (Art. N2, para. 1, point (a), AML Law). European companies (*sociétés européennes* – SE), European cooperative societies (*sociétés coopératives européennes* – SCEs), and European Economic Interest Groupings (EEIGs) are regulated by the relevant specific European provisions (Regulation 2137/85 for EEIGs; Regulation 2157/2001 for SEs and Regulation 1435/2003 for SCEs), and for other aspects by the provisions of the Belgian Companies and Associations Code (CSA) applicable to companies incorporated under Belgian law (Art. 1:35).

(b) *Foundations* (private foundations (*fondations privées* – FP) and public-interest foundations (*fondations d'utilité publique* – FUP)) are subject to the same transparency requirements as companies (Art. 1:35, CSA).

(c) With regard to *other legal entities*, the provisions of Art. 1:35 CSA apply to associations (non-profit organisation (*associations sans but lucratif* – ASBL) and international non-profit associations (*associations internationales sans but lucratif* – AISBL)).

[292] R.24 has been reassessed because of the changes made to the FATF standards, for which Belgium has not previously been assessed.

(d) Belgium has not taken sufficient measures to ensure that the requirements of criteria c.24.3 (b) and c. 24.10 are applied by the competent authorities to foreign legal entities posing ML/TF risks and which have sufficient links with Belgium[293] (see under the relevant criteria).

Criterion 24.2 –

(a) and **(b)** The different types, forms and characteristics of legal entities, as well as the procedures for creating them, are identified and can be consulted in the CSA (Art. 1:1 to 1:7 and Book 2). This information is published on the *Moniteur Belge* (Belgian Official Journal) website and also on the websites of various government departments (e.g. SPF Justice and SPF Economy).[294]

(c) The mechanisms for obtaining and keeping basic information on legal entities and their beneficial ownership (BO) are available from the Banque-Carrefour des Entreprises and the "Ultimate Beneficial Owners" (UBO) register (Art. III.29 of the Code of Economic Law (CDE) and Art. 6 et seq. of the Royal Decree (RD) of 30 July 2018 on the operating procedures for the UBO register). This information is published on the website of the Banque-Carrefour des Entreprises register and SPF Finance.[295]

Criterion 24.3 –

(a) Belgium has carried out a cross-sectorial assessment of the ML/TF risks to which legal entities and arrangements are exposed, which was updated in 2024. It was based notably on the ML NRA, the European Commission's supranational ML/TF risk analysis and data provided by the Federal Police Criminal Investigation Department (Police Judiciaire Fédérale – PJF), the CTIF and SPF Economy. The prosecuting authorities were not involved.

The risks associated with legal entities and their abuse have been identified as a major ML risk. This cross-sectorial assessment covers the different types of legal entities created in Belgium but establishes that the main risks are not specific to a different form of legal entity. The analysis of the TF risk is less substantiated because information concerning the involvement of legal entities in terrorist financing is limited as their role in TF schemes is considered as secondary in investigations.

Belgium has implemented certain measures to mitigate the ML/TF risks identified (e.g. controls/deregistration of shelf companies from the Banque-Carrefour des Entreprises and the UBO register (see IO.5). Reforms introduced by the Belgian Companies and Associations Code (Code des sociétés et des associations – CSA) in 2019 have contributed to increasing the vulnerability of legal entities, especially by easing the conditions for their creation, and, as a consequence, for the creation of the shell companies that may be used in ML schemes.

(b) The analysis of the ML/TF risks posed by foreign legal entities with links to Belgium is in its infancy. Belgium has identified the forms and countries of origin of these entities and, in the cross-sectional analysis of legal entities, reports the beginnings of an analysis based on CTIF and police data on the involvement of these entities in ML investigations. Belgium has not carried out a more in-depth analysis to identify the specific ML/TF risks and typologies they present, nor has it implemented specific measures to mitigate and manage these risks.

Criterion 24.4 – All companies created in Belgium and subject to the CSA are registered in the Banque-Carrefour des Entreprises, which is the register of Belgian companies and legal entities (Art. III.16 CDE). The basic information set out in criterion 24.5(a) can be consulted on the website of the Banque-Carrefour des Entreprises and the *Moniteur belge* websites (Articles III.31 CDE and 2:14 CSA). Access to certain some

[293] This includes legal entities that have a branch or establishment in Belgium, as well as those that carry out activities subject to Belgian VAT and Belgian social security, participate in public contracts in Belgium or rent real estate in Belgium.

[294] Sociétés, associations et fondations | Service public fédéral Justice (belgium.be) ; Starting a business | FPS Economy (fgov.be) and Accredited business counters | FPS Economy (fgov.be)

[295] Banque-Carrefour des Entreprises | FPS Economy (fgov.be); FPS Finances.

information may be subject to authorisation from the Minister for the Economy (Art. III.30 CDE), but no data currently falls within the scope of this provision.

Criterion 24.5 –

(a) When registering with the Banque-Carrefour des Entreprises, legal entities must provide the information required by this criterion. (Art. 2:8 CSA for companies, Art. 2:9-2:10 for associations and 2:11 for foundations; Art. III. 17 and III. 18, CDE).

(b) All limited liability companies existing in Belgium must keep a separate register for each class of registered securities that they are authorised to issue (shares, including classes of shares and associated voting rights, participation certificates and bonds) (Art. 5:24 to 5:28 CSA for SRLs, Art. 6:24 to 6:26 CSA for SCs and SCEs, and Art. 7:28 to 7:32 CSA for SAs and SEs). The name and number of shares of partnerships are set out in their articles of association (Art. 2:8, para.2, sub-para. 4 and 6 CSA). Information concerning the holder(s) of dematerialised securities is held by the authorised account keeper (Art. 5:30 CSA for SRLs, Art. 6:29 CSA for the SCs/SCEs and Art. 7:35 CSA for the SAs/SEs). ABSLs must keep a register of their members (Art. 9:3 CSA). For AISBLs, the names of the founders and directors must be stated respectively in the articles of association and the instruments of appointment (Art. 2:10, para.1, para.4 and para.2, sub-para. 1 CSA). A foundation under Belgian law has neither members nor associates, but the name of each founder and director must be stated in its articles of association (Art. 2:11 para.1, sub-para. 4 and para.2, sub-para.8 CSA).

(c) In principle, the registers are kept at the company's registered office (Art. 5:24 CSA for SRLs, Art. 6:24 CSA for SCs and SCEs, and Art. 7:28 CSA for SAs and SEs). Companies may decide to split a register in two, with one part being kept outside the registered office, in Belgium or abroad. In this case, a copy of each part is kept in the location at which the other part is filed. The company must announce the location of the second part of the register by publication in the Annexes to the Belgian Official Journal (Art. 5:28 CSA for SRLs, Art. 6:26 CSA for SCs and SCEs and Art. 7:33 CSA for SAs and SEs). This requirement could affect companies' ability to provide information held outside the company's registered office quickly and upon request. This failure is mitigated by the fact that the UBO register holds information on beneficial ownership (BO) in the country (see C. 24.6 (b) (i)).

In the case of ASBL, the register of members must be available for consultation at the association's registered office (Art. 9:3 CSA). With regard to partnerships, AISBLs and foundations, the articles of the CSA do not specify that the articles of association of the said legal entities must be kept at their registered office. However, the information is kept by the registries of the company's courts in whose territorial jurisdiction the company’s registered office is located, and by the Banque-Carrefour des Entreprises (Art 2:7, 2:9, 2:10, 2:11 and 2:23 CSA).

Criterion 24.6 – Belgium has several mechanisms in place to ensure that information on the beneficial ownership of legal persons can be determined in a timely manner by a competent authority:

(a) Companies and other legal persons are required to collect and maintain adequate, accurate and up-to-date information on their beneficial ownership and to transmit this information to the UBO register (with the exception of companies listed on a regulated market) and to reporting entities where business relationships are established (Art.1:35 CSA). Belgian legislation does not expressly require legal persons to cooperate with IFs and DNFBPs to determine their beneficial owners.

(b) (i) Belgium has established a centralised beneficial ownership register (UBO register), whose purpose is to provide access to adequate, accurate and up-to-date information on the beneficial owners of companies, foundations and (international) non-profit organisations (Art. 73-74, AML Law). The requirement to provide information on beneficial owners does not apply to companies listed on a regulated market, but this is offset by the specific financial reporting and disclosure requirements to which such companies are subject (see Criterion 24.1 (c)).

The UBO registry has been operational since September 2018 and has a solid architecture. It is overseen by SPF Finance, which is responsible for managing, collecting, storing and checking the quality of the information provided by legal entities, as well as making information on beneficial owners available via the UBO register.

(ii) *(Not applicable)*

(c) Legal persons who have a bank account in Belgium or in a banking institution located in the EEA (Directive 2015/2366) must provide information about their beneficial owners to banking institutions under the customer due diligence measures (Art. 5, para 1, 19 and 23 AML Law). This requirement does not apply where legal entities do not have an account in Belgium or the EEA. In addition, a register called the Central Point of Contact (PCC) for financial accounts and contracts is kept by the National Bank of Belgium and centralises banking information relating to financial accounts and contracts existing in Belgium (see R.31). The PCC provides access to information that can help to identify beneficial owners.

Criterion 24.7 –Legal persons are not required to maintain the basic and beneficial ownership information required under criteria 24.5 and 24.6 after being dissolved. This information is kept by the Banque-Carrefour des Entreprises and the UBO registers for thirty and ten years respectively after the date on which the legal entity ceased to exist (Art. III.18, §4 CDE, Art. 75 AML Law and Art. 25 Royal Decree 2018). Lastly, obliged entities are required to keep documents and information relating to the identity of their customers and their BOs for a period of ten years from the end of the business relationship or the execution of the transaction in the case of occasional customers (Art. 60 AML Law, see C. 11.1).

Criterion 24.8 –

Satisfactory information - The scope of the basic information held by legal entities and required for registration with the Banque-Carrefour des Entreprises is sufficient to verify the legal existence of legal entities (Art. III.18 CDE, C. 24.5 a). When registering in the UBO register, legal entities must provide, by electronic means, adequate, accurate and up-to-date information on their beneficial owners (name, date of birth, nationality, country and address of residence, national identification number[296] and nature and extent of interests held) (Art. 3 Royal Decree 2018,[297] pursuant to Art. 73-75 of the AML Law and Art. 1:35 CSA).

Accurate information - A notary's services are required for the creation and subsequent modification of five of the nine forms of companies, including some of the most common and highest-risk forms, (i.e. the SRL and the SA). The creation of three types of non-profit entities also requires a notarial deed (i.e. AISBL, FP and FUP). As obliged entities, notaries are subject to AML/CFT due diligence obligations. However, a notary's services are not required for four forms of companies, including SNCs and Scomms, as well as for the ASBL, which are created by private deed, despite the ML/TF risks identified.

The clerks of the Commercial Courts are responsible for encoding the basic information relating to entities in the Banque-Carrefour des Entreprises. The circular of 23 October 2023 requires the clerks to verify the identity of the applicant and partners with unlimited liability, as well as to consult the register *JustBan*, which records court decision prohibiting individuals from holding managerial functions. Otherwise, the registry's checks are purely formal and no provisions require them to check the other basic information to be recorded. Furthermore, the Circular only covers paper filings and does not address the checks to be carried out for electronic filings via *JustAct* (the former eGreffe application) and eDepot.

There is no requirement for the business counters (*guichets d'entreprises*) that register certain categories of legal entity to carry out verification measures (see IO.5). Consequently, the measures to verify the accuracy of the basic information required for the formation of legal entities created under private deed are limited.

[296] The identification number in the Belgian National Register of Natural Persons or the *Banque-Carrefour pour la Sécurité Sociale* and, where applicable, any similar identifier given by the State in which the beneficial owner resides or of which he or she is a citizen.

[297] Royal Decree on the operating procedures for the UBO register.

The UBO register unit at SPF Finance is responsible for monitoring compliance with the obligation to disclose information on beneficial owners and for monitoring the quality of the information in the UBO register (Art. 74 AML Law).

Up-to-date information - The basic information recorded in the Banque-Carrefour des Entreprises register must be updated without delay after any change (Art. III. 18 para. 3, CDE). The competent authorities are required to notify the Banque-Carrefour des Entreprises register as soon as they notice any error in the information or any information missing from the register (Art. III.38, §2 CDE).

Legal entities are required to transmit information concerning their BO to the UBO register one month after their creation and to notify the register of any changes without delay (Art. 1:35 CSA, Art. 21. 7°, Royal Decree 2018). The information recorded must be confirmed every year (Art. 5, Royal Decree 2018). When requested by SPF Finance, following a discrepancy report from obliged entities, the competent authorities or legal representatives have one month to respond (Art. 74/1, AML Law).

A mechanism for interconnecting data from the UBO register with data from other national databases (i.e. Banque-Carrefour des Entreprises, the Belgian National Register of Natural Persons and the *Banque-Carrefour de la Sécurité Sociale* (BCSS), enables the BO-related information in the UBO register to be updated automatically when changes are made to the related national databases[298] (Art. 24, § 2, 1° Royal Decree 2018). This interconnection does not always enable the cross-referencing of information relating to foreign beneficial owners, except where an identifiable link with Belgium led to their registration in the national databases.

Obliged entities and other authorities, including tax authorities, must report any discrepancies between the information recorded in the Banque-Carrefour des Entreprises and UBO registers and the information obtained during the course of their due diligence (Art. 74/1, 2017 AML Law).

Criterion 24.9 –The competent authorities can access information about beneficial owners in a timely manner by directly consulting the UBO register (Art. 75 para. 2, AML Law). They can also access basic information about companies and other legal persons listed in the Banque-Carrefour des Entreprises and published in the *Moniteur belge* (see C.24.4 and 5). In addition, the competent authorities can quickly and effectively access information held by Belgian banking institutions centralised at the PCC (see R.31).

Criterion 24.10 – The Belgian competent authorities can access information on beneficial owners when a foreign legal person controls a Belgian entity which is itself required to submit this information to the UBO register, when it holds a bank account with a Belgian banking institution, and via the Beneficial Ownership Register Interconnection System (BORIS) for the interconnection of beneficial ownership registers with certain EU countries, which allows the Treasury Administration to collaborate and exchange information with the managers of similar registers in other EU Member States (Art. 75 AML Law, Art. 2:24, 2:25 and 2:26 CSA, Art. 17, §2 para. 4, Royal Decree 2018).[299]

However, no mechanism provides access to information for other foreign legal entities from EU countries that do not (yet) participate in BORIS, or those established outside the EU and identified as having an adequate link with Belgium (see C. 24.1. d))

Criterion 24.11 –The basic information listed in Criterion 24.5(a) on companies and other legal entities entered in the Banque-Carrefour des Entreprises register can be accessed by obliged entities and competent foreign authorities via the *Moniteur belge* and the Banque-Carrefour des Entreprises website (see c.24.4)

[298] Respect for the protection of personal data in the context of national database interconnection mechanisms is governed by the provisions of Article 17, §2 and Article 24 of the UBO Royal Decree 2018.

[299] Respect for personal data protection in the context of national database interconnection mechanisms is governed by the provisions of Article 17, §2 and Article 24 of the Royal Decree on UBO, 2018.

Criterion 24.12 – Since the abolition of bearer shares, which became fully effective on 1st January 2014, issuers have been exclusively using registered or dematerialised securities.[300]

Criterion 24.13 – Belgium does not prohibit or regulate the use of nominees directors. The mechanisms in place are insufficient to ensure that shares registered in the name of nominees or directors acting on behalf of another person are not misused despite the revision of the CSA.

(a) SRLs and SAs may issue registered or dematerialised shares, recorded in the name of nominee shareholders. An issuer acting on behalf of another person, which may be a legal entity, is required to declare its status and the identity of the certificate holder to the issuing company and to the relevant securities register, but not to the UBO register (Art. 5:49 and 7:61 CSA). This information is not made public.

A second mechanism requires a legal entity holding a position as a member of an administrative body or as a delegate responsible for day-to-day management to appoint a natural person ("nominee director") as its permanent representative responsible for carrying out this mandate (Art. 2:55 CSA). These provisions provide for the publication of these designations[301]/cessations.

Shares in Belgium may be registered in the name of nominees under a nominee agreement. However, the identity of the person actually holding the shares, the status of the nominee and his or her identity do not appear either in the public registers or in the register kept by the company. This lack of publication makes it difficult to verify the shareholder's status.

(b) Belgium does not apply the mechanisms set out in sub-criterion 24.13 (b).

(c) Belgian law does not prohibit the use of proxy shareholders or directors.

Criterion 24.14 – Financial penalties are imposed on legal entities that fail to meet their obligations under R.24. The range of these penalties allows for the imposition of proportionate penalties (Art. XV.77. 1° Art. XV.70 2° and XV.60/20 CDE, and Art. 132, para. 6, AML Law). The same observation applies to the penalties incurred by natural persons individuals for failure to their declare beneficial ownership (Art. 1:36 CSA). However, no financial penalties are applied to natural persons in respect of basic information obligations.

Other sanctions against legal entities include the automatic removal from the register of any entities that do not comply with their obligations regarding the UBO register (Art III.42, §1, al. 6, CDE). Civil and criminal penalties are imposed in the event of abuse of the nominee mechanism: (Art. 5.39 CC – Art. 196 CP – five to ten years' imprisonment for forgery of documents). No penalties are imposed for failure to comply with the obligation imposed on legal entities to retain documents covered by R.24.

Criterion 24.15 – Belgium has a legal framework for providing international cooperation on basic information and on beneficial owners in accordance with Recommendations 37 and 40 as follows:

(a) There are no unduly restrictive legal conditions on exchanges of information or international mutual assistance likely to hinder access to information on beneficial owners.

(b) Competent foreign authorities may access the basic information held by the Banque-Carrefour des Entreprises, which can be accessed directly online (Art. III.29, para. 1 and Art. III 31 CDE).

(c) There are no obstacles to access by foreign authorities to shareholder information held by companies.

(d) The Belgian competent authorities obtain information on beneficial owners on behalf of counterparts in EU member countries with which they have concluded cooperation agreements (Art. 12 para.3 Royal Decree 2018). There is no legal basis for the Belgian authorities to obtain this information on behalf of non-European counterparts, which must submit a request to SPF Finance and demonstrate a legitimate interest in accessing

[300] See Belgium MER (2015), p. 267.

[301] A deed of appointment filed with the clerk of the competent court is required, as well as publication in the *Moniteur belge* and registration with the Banque-Carrefour des Entreprises.

the information (Art. 10, Royal Decree 2018). The concept of legitimate interest is sufficiently broad to allow foreign judicial authorities to access this information.

(e) Certain authorities (CTIF and SPF Finance) have put in place mechanisms to monitor the quality of assistance received from other countries with regard to basic information and beneficial ownership. There is no systematic and structured system for monitoring the quality of responses obtained in the framework of international mutual assistance in criminal matters at the level of the Belgian judicial and supervisory authorities, which could be used to specifically monitor the follow-up of requests for assistance issued in order to locate beneficial owners residing abroad.

(f) Belgium keeps and provides easy access to information that can be used to identify beneficial owners in the UBO register. Information on beneficial owners obtained from foreign authorities cannot be accessed by the Belgian authorities other than the SPF Finance agents responsible for managing the UBO register.

(g) The agency in charge of maintaining the UBO register – i.e. SPF Finance – is responsible for responding to any request for information about beneficial owners if the person making the request has a legitimate interest in obtaining this information (Art. 75 para.2, AML Law; Art.6 et seq., Royal Decree 2018). However, the responsibility of SPF Finance for international requests for mutual assistance has not been clearly established, and Belgium has not taken any steps to publicise its role.

Weighting and conclusion – Interconnected mechanisms are in place to provide the Belgian authorities with timely access to accurate and up-to-date beneficial ownership information held by the UBO register. However, there is no requirement to verify the accuracy of all basic information for the formation of legal entities created by private deed. This shortcoming is significant given the risk of abuse for ML purposes identified by Belgium with regard to Scomm, SNC and ASBL The mechanisms in place are insufficient to ensure that shares registered in the name of nominees or directors acting on behalf of another person are not misused. The reform of the Belgian Companies and Associations Code (Code des sociétés et des associations – CSA) in 2019 has also contributed to increasing the vulnerability of legal entities, especially by easing the conditions for their creation which, in the absence of provisions providing for sufficient control of basic information at the registration stage, facilitates the creation of shell entities and shell companies. The analysis of ML/TF risks posed by foreign legal entities with links to Belgium is in its infancy, which is a significant factor given the open nature of the Belgian economy and the scale of the financial and non-financial flows to which Belgium is exposed. In addition, the prosecution authorities were not involved in developing the cross-sectorial assessment of ML/TF risks for legal persons. These shortcomings are part of a context in which the abuse of legal entities for ML purposes has been identified as a high risk by Belgium. **Belgium is partially compliant with R.24.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements[302]

Recommendation 25 has been reassessed in the light of the amendments made by the FATF in February 2023, which significantly recast the requirements relating to the transparency of legal arrangements.

Belgium was rated largely compliant in the 2015 MER because of the inadequacy of mechanisms to ensure that beneficial ownership information is accurate and kept up to date, and the lack of a clear policy on penalties applicable to professional trustees who fail to comply with their AML/CFT obligations, which makes it impossible to characterise their proportionality.

Criterion 25.1 – Belgian law does not permit the creation of express trusts and *fiducies*, and Belgium has not ratified the Hague Convention. However, the requirements of R.25 apply to all foreign legal arrangements administered in Belgium,[303] including trusts (defined in Art. 4. 26° AML Law), *fiducies* and other similar legal arrangements (Art. 74 para.1 AML Law; and Art. 4 §2 Royal Decree of 30 July 2018 on the operating procedures of the UBO register "RD July 2018").

Criterion 25.2 – Belgian law does not provide for express trusts or *fiducies* to be governed by Belgian law.

Criterion 25.3 –

(a) Belgian law does not provide for express trusts or *fiducies* to be governed by Belgian law.

(b) and (c) The ML NRA has not identified any significant specific risks associated with legal arrangements in Belgium. The analysis of ML/TF risks posed by legal entities in 2024 includes brief descriptions of the theoretical risks associated with legal arrangements in general, which are not specific to Belgium. However, the analysis does not include a specific assessment of the risks associated with the various types of trusts and other legal arrangements administered in Belgium by a Belgian resident, nor the forms of foreign legal arrangements with sufficient links to Belgium. General risk mitigation measures have been taken, including the obligation for trusts and similar legal arrangements governed by foreign law and administered in Belgium to register with the UBO and the Banque-Carrefour des Entreprises (Art. 4, §2 RD 2018).

Criterion 25.4 –

(a) Trustees, fiduciaries and persons occupying an equivalent position are bound by similar obligations in respect of trusts/*fiducies*[304] that they administer from Belgium (Art. 4 RD 2018). This information includes the various elements required by C.25.4 (a).

(b) Trustees and equivalents are required to obtain and hold satisfactory, accurate and up-to-date information concerning the beneficial owners of trusts, *fiducies* or other similar legal structures which are legal persons or legal arrangements (Art. 4.§ 1 RD 2018). Any natural person who has ultimate control over a trust or *fiducie* by virtue of being its direct or indirect owner or by other means, is considered to be a beneficial owner (Art. 4 para. 27(b) AML Law). Trustees are required to obtain and hold satisfactory, accurate

[302] R.25 has been reassessed because of the changes made to the FATF standards, for which Belgium has not previously been assessed.

[303] This includes trusts, *fiducies* and any other similar legal arrangements under foreign law administered by a Belgian resident (trustee or fiduciary), property or rights in Belgium that are placed in a trust under foreign law and where a person domiciled in Belgium may have the status of settlor or beneficiary of a trust under foreign law (Art. 4 para.2 RD 30 July 2018, Chapter XII Belgian Code of Private International Law). Trusts and similar foreign legal arrangements may also have effective control over a Belgian legal entity.

[304] In the case of trusts and *fiducies*, the following are considered to be beneficial owners: (i) the settlor(s); (ii) fiduciary (fiduciaries) or trustee(s); (iii) protector(s), where applicable; (iv) beneficiaries and any other natural person exercising ultimate control over the *fiducie* or trust by virtue of being its direct or indirect owner, or by other means. For legal arrangements similar to *fiducies* or trusts, the beneficial owners are the natural persons occupying functions equivalent or similar to those of the persons mentioned below (Art. 4 para. 27, AML Law of 2017).

and up-to-date information concerning the parties to trusts or other similar legal arrangements which are legal persons or legal arrangements (Art. 75§ 1er, 6, AML Law).

(c) Belgian legislation does not impose an obligation for trust administrators, fiduciaries and persons occupying an equivalent position in a similar legal arrangement, who are resident or administer an express trust or similar legal arrangement in Belgium, to hold basic information on other regulated agents and service providers of the trust or similar legal arrangement.

Criterion 25.5 – As obliged entities under the AML law, trustees, fiduciaries and persons occupying an equivalent position in a similar legal arrangement are required to keep the information referred to in C.25.4 for a minimum period of ten years after the end of their involvement in the trust or similar legal arrangement (see C. 22.2 and R.11).

Criterion 25.6 – Administrators of trusts and equivalents are required to ensure that the information they hold in accordance with C.25.4 is accurate and up to date and that the information they transmit to the register of beneficial owners of trusts, *fiducies* or other legal arrangements (UBO register, see R.24) is updated within one month of any change (Art. 4 para.1, sub-para.12, RD 2018). The absence of an obligation to hold the information referred to in C. 25.4(c) has an impact on the rating of this criterion.

Criterion 25.7 –

(a) Trust administrators and fiduciaries are required to declare their status to the reporting entities when, in their capacity as trustee or fiduciary, they enter into a business relationship or carry out an occasional transaction involving an amount in excess of the legal thresholds (Art. 4 para. 4, RD 2018).

(b) Trustees/fiduciaries/other equivalent persons who are subject to the AML Law are under an express obligation to cooperate with the competent Belgian authorities (Art. 63 and 81 AML Law). Trustees/fiduciaries/other equivalent persons not subject to the AML Law are not legally subject to the same requirements. However, no provisions restrict their ability to provide the necessary information to the competent Belgian authorities. "Foreign" trusts/legal arrangements administered by Belgian trustees or equivalents must be registered in the Banque-Carrefour des Entreprises and UBO registers (Art. 4 para.1 RD 2018). Access to basic information and information on the beneficial owners of trusts and *fiducies* administered in Belgium can be obtained by consulting the information in the Banque-Carrefour des Entreprises and UBO registers to which the competent authorities have access (Art. 7 RD 2018).

(c) There is no impediment to providing information on trusts and any other similar foreign legal arrangements to reporting entities, given the obligation incumbent on trustees to identify their customers and be aware of the nature of the business relationship (Art. 26 para. 2 AML Law, see R.10).

Criterion 25.8 –

Satisfactory information - The scope of the information on the beneficial owners of trusts, fiducies and similar legal arrangements in accordance with criteria c.25.4 (a) and (b) is sufficient (Art. 4 Royal Decree 2018). Information on trustee status for FIs and DNFBPs is generally satisfactory (c 25.7 (a)). Finally, trusts/fiducies are subject to the obligation to provide basic information on beneficial owners and assets to the Banque-Carrefour des Entreprises and UBO registers (Art. 4 § 2 of the Royal Decree of 30/07/2018 - see c. 25.9).

Accurate information - When registering with the UBO register, trusts and legal arrangements are required to provide documentary evidence of the details registered under the control structure of a trust or similar legal arrangement (Art. 4 para.1 RD 2018). SPF Finance is responsible for collecting, storing, managing and controlling the quality of the information in the UBO register (Art. 74 § 2 of the AML Law). The interconnection of the UBO register with the national databases enables the information to be updated when these databases contain information on those legal arrangements (Art. 24 RD of July 2018). SPF Finance may also cross-reference the information in the UBO register with that held by the Land Registry concerning trustees or fiduciaries who own real estate in Belgium (Art. 79 §6 AML Law, Art. 17 RD UBO 2021/8)

Obliged entities must verify the accuracy of the declarations provided by trustees and fiduciaries when verifying information relating to their customers (Art. 27 AML Law)

Up-to-date information - Information on the beneficial owners of registered legal arrangements must be corrected or deleted from the UBO register without delay as soon as changes are made (Art. 21 RD 2018). The recorded information must be confirmed every year (Art. 5 RD 2018) and trusts and other similar legal arrangements are required to rectify or delete inaccurate recorded data within one month (Art. 4, §2 3° and 21 RD 2018). Trustees/fiduciaries have one month to respond to any request from the Treasury Administration when it takes steps to verify the adequacy, accuracy and currency of the information recorded on the beneficial owners of trusts/*fiducies*, particularly following a report from obliged entities (Art. 74/1 AML Law).

Obliged entities and other authorities, including tax authorities, must report any discrepancies between the information recorded in the UBO register and those obtained during the course of their due diligence (Art. 74/1 2017 AML Law).

Criterion 25.9 –

(a) The Belgian competent authorities have access to basic information and information on the beneficial owners of trusts, *fiducies* and similar legal arrangements administered in Belgium, via the Banque-Carrefour des Entreprises and UBO registers (Art. 7 RD 2018). Foreign legal arrangements falling within the definition of Art. 4 of the Royal Decree of July 2018 that are already registered in another EU Member State are not required to register in the UBO register, and provide an extract of the information transmitted to the foreign register (Art. 4 para. 3 RD 2018).

(b) Information on the beneficial owners of legal arrangements administered in Belgium may be made available to the competent authorities by the tax authorities (Art. 307 para. 1, sub-para. 4 of the Income Tax Code). Information on trust assets is also available from the Central Point of Contact (PCC) for Financial Accounts and Contracts (see R.31).

(c) Finally, information relating to legal structures may be obtained from entities subject to the AML Law (Art. 63 and 81, AML Law).

Criterion 25.10 – The Belgian criminal justice authorities and the CTIF are empowered to access the information required under (a), (b) and (c) from various registers and entities subject to the AML Law. They have direct access to information held by the Banque-Carrefour des Entreprises and UBO registers, including information on beneficial ownership and the residence of the trustee/fiduciary (Art. 75 AML Law 2017, Art. 4 RD 2018). Obliged entities must provide information on their customers, including with regard to legal arrangements (Art. 63 and 81 AML Law 2017). Information about the assets held can also be obtained by consulting the PCC.

Criterion 25.11 –

(a) The responsibility for complying with the obligations of the Interpretative Note to R.25 is set out in Article 4 AR 2018.

(b) Failure to comply with the obligations laid down by R.25 exposes trust administrators and trustees to administrative penalties of between EUR 250 and EUR 50,000 (Art. 132, para. 6 AML Law, Art. 18 RD 2018). The range of these penalties allows for the imposition of proportionate penalties. Since the end of 2023, the authorities have also been empowered to request the ex officio revocation of all trusts/*fiducies* and similar legal arrangements that do not fulfil their obligations (Art III.42, §1, paragraph 6 of the CDE).

(c) There are no provisions to sanction failure to make the information referred to in criteria 25.4 and 25.5 available to the competent authorities in a timely manner.

Criterion 25.12 – Belgium has established the legal framework to cooperate with foreign authorities regarding trusts, *fiducies* and any other legal arrangements, including information on beneficial owners in accordance with Recommendations 37 and 40, in the following manner:

(a) there are no obstacles likely to impede access to information on the beneficial ownership of legal arrangements by the competent foreign authorities;

(b) the competent foreign authorities have access to basic information on the legal arrangements recorded in the Banque-Carrefour des Entreprises register. A request to consult the information in the UBO register must be submitted to SPF Finance and the authorities must demonstrate a legitimate interest in accessing such information (Art. 10 Royal Decree 2018). The concept of legitimate interest is sufficiently broad to allow foreign judicial authorities to access this information - see C. 24.15 (a).

(c) The Belgian authorities may exchange information on trusts and legal arrangements at national level (Art. 63 AML Law).

(d) The Belgian competent authorities obtain information on beneficial owners on behalf of counterparts in EU member countries with which they have concluded cooperation agreements (Art. 12 para.3 RD 2018). There is no legal basis for the Belgian authorities to obtain this information on behalf of non-European counterparts, which must submit a request to SPF Finance and demonstrate a legitimate interest in accessing the information (see c.24.15 (d)).

(e) The agency in charge of maintaining the UBO register – i.e. SPF Finance – is responsible for responding to any request for information about beneficial owners if the person making the request has a legitimate interest in obtaining this information (Art. 75 para.2, AML Law; Art.6 et seq., Royal Decree 2018). However, the responsibility of SPF Finance for international requests for mutual assistance has not been clearly established, and Belgium has not taken any steps to publicise its role. Belgium ensures easy access through the UBO register to the information held to identify the beneficial ownership of trusts and similar legal arrangements. Information obtained from foreign authorities cannot be accessed by the Belgian authorities other than the SPF Finance agents responsible for managing the UBO register.

> ***Weighting and conclusion*** – Belgium has not identified any significant specific risks associated with trusts and legal arrangements in Belgium. However, the analyses carried out are still in their infancy and relatively theoretical. **Belgium is largely compliant with R.25**.

Recommendation 26 – Regulation and supervision of financial institutions[305]

Belgium was deemed partially compliant with R.26 in the 2015 MER. The identified shortcomings mainly concerned the risk-based approach applied by the main supervisory authorities for the financial sector (BNB, FSMA). R.26 was reviewed in the 2018 Follow-Up Report and the rating was reassessed as compliant.

Criterion 26.1 – The scope of application of the AML Law includes all the financial institutions covered by the FATF Glossary. The 2010 reform of the architecture of financial sector supervision led to a new division of responsibilities, now shared between the National Bank of Belgium (BNB) and the Financial Services and Markets Authority (FSMA). Insofar as AML/CFT supervision is integrated into prudential supervision, the BNB and the FSMA are respectively responsible for AML supervision and regulation of the institutions under their prudential responsibility. Consumer credit companies and finance lease companies are supervised by SPF Economy. The scope of the law is extended to the National Bank of Belgium (BNB) in order to define a

[305] Mutual Evaluation Report (2025) and Follow-up Report for Belgium (2018)

comprehensive and effective AML/CFT framework. This institution is placed under the authority of the Minister for Finance. For its own-account financial activities (e.g. postal payments/money orders, distribution of prepaid cards), Bpost is subject to the AML Law and is placed under the supervision of SPF Finance. However, it is not directly subject to AML/CFT obligations in respect of activities carried out in its capacity as an agent of a credit institution and a European payment institution; these institutions themselves are subject to AML/CFT obligations. Bpost agent also acts as a "central contact point" under the supervision of SPF Finance, which supervises the European payment institution that carries out its activities in Belgium via the network of post office counters (see R.14).

Criterion 26.2 – All institutions subject to the Core Principles are licensed by the BNB, including institutions authorised to carry out money or value transfer operations (see R.14). The other institutions are either granted licenses or registered by the relevant supervisory authority. Furthermore, the establishment or the continued operation of shell banks is not permitted (Art. 43, Law of 25 April 2014 "Banking Law").

Criterion 26.3 – All financial institutions are subject to legislative provisions requiring them to provide information on the quality of their managers and their professional good repute when applying for licensing or registration.[306] In addition, for credit institutions, investment firms, and insurance companies, the BNB must be given prior notification of any intended change to the institution's administration, operation or effective management, and it may object to the appointment of the person in question. For insurance intermediaries and banking and investment service brokers, this notification concerns any change in the institution's control. As regards control over shareholders, when applying for licensing or registration, the supervisory authority must be sent information about holders of a significant interest which may have an influence over the control of these financial institutions.[307] The supervisory authority may deny a license or registration if it considers that the persons in question lack the necessary capacities to ensure the sound and prudent management of the institution. For credit institutions and investment firms, management companies of collective investment funds, insurance companies, electronic money institutions and clearing institutions, ongoing supervision of shareholders also applies and involves prior notification of acquisitions, increases, reductions and disposals of qualified interests in a financial institution. The supervisory authority may object to the acquisition if it has reasonable grounds to consider that the proposed acquirer lacks the necessary capacities to ensure the sound and prudent management of the financial institution. These financial institutions must also give notice of acquisitions concerning non-qualified interests and make occasional and periodic declarations of acquisitions of securities which go beyond the thresholds applicable to prior notifications, thus giving the supervisory authority ongoing knowledge of the shareholding structure.

Criterion 26.4 – The AML Law stipulates that supervision is carried out on the basis of a risk assessment (Art. 87 §1), which takes account of the national ML/TF risk assessment as well as the supranational assessment carried out at European level, and the frequency and extent of on-site and off-site supervision are based on the entity's risk profile. The general supervisory framework in force in Belgium nonetheless provides that the responsible authorities must take risk factors into account:

(a) BNB regulation and supervision of financial institutions subject to the Core Principles are based on the Basel Committee on Banking Supervision Principles, and on the Principles of the International Organisation of Securities Commissions and of the International Association of Insurance Supervisors. All of these financial institutions are subject to prudential supervision according to a risk-based approach. AML/CFT supervision, including the application of consolidated supervision of the group, is carried out within the framework of

[306] Notably Art. 19 and 20 Law of 25 April 2014; Art. 8 and 90 Law of 9 July 1975; Art. 59 to 61 Law of 6 April 1995; Art. 62 Law of 21 December 2009.

[307] Art. 18 and 46 to 54 Law of 25 April 2014; Art. 67 and 67 *bis* Law of 6 April 1995; Art. 207 and 208 Law of 3 August 2012; Art. 23 and 24 Law of 9 July 1975.

global oversight of financial institutions but may be supplemented by specific AML/CFT compliance inspections.

(b) The AML Law of 2017 provides powers for SPF Finance and SPF Economy to exercise control over the institutions under their jurisdiction for compliance with AML/CFT obligations.

Criterion 26.5 – The frequency and extent of on-site and remote AML/CFT inspections of financial institutions or financial groups is determined on the following bases (Art. 87 AML Law):

(a)-and **(b)** the entity's risk profile, resulting from a combination of (1) an assessment of the ML/TF risks to which the obliged entity is exposed, taking account of the characteristics of its business sector, the geographical areas in which it operates and its distribution channels, and (2) an assessment of the management of these risks, which includes an assessment of the measures it has taken to identify and reduce its risks, and an assessment of its level of compliance with applicable legal and regulatory obligations.

and **(c)** a risk assessment that takes account of the national ML/TF risk assessment and the supranational assessment carried out at European level.

Criterion 26.6 – The supervisory authorities must review the risk profile of reporting entities periodically, at a frequency appropriate to the sector of activity and the previous risk profile, but also when significant events occur that are likely to affect the level of the entity's ML/TF risks or the level of management of these risks (Art. 87 AML Law).

> *Weighting and conclusion* – **Belgium is compliant with R.26.**

Recommendation 27 – Powers of supervisors[308]

Belgium was deemed largely compliant with R.27 in the 2015 MER. The main shortcomings identified concerned the sanctions applicable by SPF Economy and SPF Finance, which were limited to the publication measures and administrative sanctions provided for in the AML/CFT Law. R.27 was reviewed in the 2018 Follow-Up Report and reassessed as compliant.

Criterion 27.1 – The BNB and the FSMA, as well as the other financial sector supervisory authorities, have general powers to control or supervise financial institutions.[309] The AML Law also grants the BNB and the FSMA specific powers, which include imposing administrative penalties, i.e. publishing decisions taken and/or imposing an administrative fine of a minimum of EUR 250 and a maximum of EUR 1,250,000 (Art. 91 - 113). Similar powers are granted to SPF Economy (Art. 107 and 108 AML Law).

Criterion 27.2 – The AML/CFT Law grants supervisory authorities power to conduct on-site inspections (BNB: Art. 91, para.2, FSMA: Art. 99, para.3, SPF Finance/Treasury: Art.110, para.2, SPF Economy: Art. 107 AML Law and XV.3 of the Belgian Code of Economic Law).

Criterion 27.3 – The AML/CFT Law grants supervisory authorities the power to obtain all the information they consider useful concerning the way these institutions implement their AML/CFT obligations. (BNB: Art. 91, para.1, FSMA: Art. 99, para.1; and Finance/Treasury: Art. 110, para.1).

Criterion 27.4 – The range of sanctions has been extended by the AML Law of 2017, which introduced additional sanction measures that include the following powers (Art. 93-96, 101-102, 108 and 112):

- issuance of an injunction requiring a natural or legal person to put an end to the behaviour in question and prohibiting it from being repeated;

[308] Mutual Evaluation Report (2025) and Follow-up Report for Belgium (2018)

[309] Such as Art. 19 and 20 Law of 25 April 2014; Art. 92 §1 Law of 6 April 1995; Art. 34 Law of 02 August 2002.

- where an obliged entity is subject to licensing: withdrawal or suspension of the licence;
- imposition of a temporary ban, for any person exercising managerial responsibilities within an obliged entity, or any other natural person held responsible for an offence, on exercising managerial functions in obliged entities.

Financial penalties are also provided for in addition to publication measures and administrative sanctions.

The BNB and the FSMA may also use the coercive measures at their disposal in the more general context of their prudential sanctioning powers[310] for the financial institutions under their supervision.

Weighting and conclusion – **Belgium is compliant with R.27**

Recommendation 28 – Regulation and supervision of DNFBPs[311]

R.28 has been reassessed to take account of the fact that company service providers are subject to the AML Law (see R.22 and 23), with an impact on the identification of the supervisory authorities for these new entities. Belgium was deemed partially compliant in the 2015 MER, due to the absence of "fit and proper" criteria for diamond dealers and estate agents, as well as shortcomings in the supervisory programmes. R.28 was reassessed in the 2018 Follow-Up Report and re-rated as largely compliant.

Criterion 28.1 –

(a) The Belgian Gaming Commission (*Commission des Jeux de hasard* – CJH), an authority governed by SPF Justice, is the authority empowered to issue casino licences. Casinos may be granted additional licences to run online casinos, for activities identical to those carried out in "physical" casinos. Foreign online casinos must hold a licence in Belgium and the CJH publishes a list of online casinos banned in Belgium.

(b) Conditions relative to the standing of managers and directors apply as regards obtaining licences, along with duties to provide shareholder information in order to determine the persons who exercise control or influence (Art. 31.4 of the law of 7 May 1999). The casino operator is required to inform the Gaming Commission of any planned changes to the personnel responsible for running the casino and to its shareholders (Art. 32.2 and 3)

(c) Persons operating games of chance, including casinos, are subject to the AML Law of 2017 (Art. 5, §1, 33°). The CJH is also responsible for the AML/CFT inspections of casinos (Art. 114 et seq. AML Law, Royal Decree of 30 October 2018, and the Law of 7 May 1999).

Criterion 28.2

The AML/CFT Law (Art. 85) designates a supervisory authority to ensure compliance with AML/CFT obligations by all other DNFBPs referred to in Article 5 (see Table 0.3, the Introduction). The authorities responsible for supervising legal and accounting/tax professions are public law institutions empowered to organise and supervise the profession by law. SPF Economy is the competent authority for company service providers, which have recently been subject to regulation, despite certain limitations noted in criterion 22.1(e).

Criterion 28.3 – The vast majority of designated non-financial businesses and professions have defined regulatory measures laying down the principle of monitoring the application of AML/CFT measures (see

[310] Such as Art. 234 §1 Law of 25 April 2014; Art. 104 §1 Law of 6 April 1995; Art. 26 §1 Law of 09 July 1975.

[311] R.28 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its 2015 Mutual Evaluation and its 2018 Follow-Up Report.

Table 0.3, the Introduction). In addition, cash transactions in excess of EUR 3,000 are prohibited in Belgium, including for dealers in precious metals.

Criterion 28.4 –

(a) The competent authorities – designated in Art. 85 – have the necessary powers to perform their duties, including powers to monitor AML/CFT compliance (Art. 87, 107 to 117 AML Law).

(b) – Verifications of good repute and integrity control measures are implemented to prevent criminals or their accomplices from accessing a management position, becoming beneficial owners or holding significant stake in a DNFBP in Belgium.

- Diamond dealers: a criminal conviction may justify a licensing refusal (RD of 20 November 2019, Art. 2).
- Company service providers (CSP) (business centres): beneficial owners must satisfy the conditions of good repute (Law of 29 March 2018, Art. 6, §3, 4°).
- Estate agents: a criminal conviction may prevent access to the profession (Law of 11 February 2013, Art. 5). With regard to estate agents operating within a company, the Law of 11 February 2013 (Art. 5, §2 and 10) limits the supervisory powers of the Belgian Professional Institute of Estate Agents (IPI), which may only exercise control over estate agents who are natural persons and who must form part of the company's management body (Art. 10, §1, 1°), but not over the beneficial owners (UBOs) of the legal entities listed in the register. In addition, in the case of legal entities engaged in the profession without being registered with the IPI,[312] in accordance with Art. 10, §2 of the same law, there is no provision for monitoring beneficial owners.
- Accounting professionals: all auditors, partners, senior managers and beneficial owners must be registered (Law of 7 December 2016, Art. 6). A criminal conviction may result in a refusal of access to the chartered accountant's and tax adviser's professions registered with the Institute for Tax Advisors and Accountants (ITAA) (Law of 17 March 2019, Art. 10, 26 and 27). An extract from the criminal record is required for directors when applying for authorisation for legal entities. The Belgian Audit Oversight Board (Collège de supervision des réviseurs d'entreprises) carries out risk-based audits.
- Lawyers: a criminal conviction may result in refusal of access to the profession or lead to disciplinary sanctions (Belgian Judicial Code, Art. 428 *bis*, 2°, a) and Art. 455).
- Notaries: only authorised professionals who meet integrity requirements may be appointed to manage a notary's office.

(c) The AML Law of 2017 provides for administrative (Art. 132-135) and criminal (136-138) penalties in the event of non-compliance with a requirement that it imposes. *Disciplinary* sanctions may also be imposed (see R.35)

Criterion 28.5 –

(a) Article 87 of the AML/CFT Law formalises the general application of the risk-based approach by the supervisory authorities for all obliged entities. The analysis in R.26 therefore applies to this Recommendation and specifies that the supervisory authorities must carry out their supervision on the basis of a risk assessment that will indicate the scope and frequency of the controls (Art. 87 § 1. 2°).

(b) The supervisory authorities must take account of the ML/TF risk profile of the entities subject to supervision (Art. 87 §12°. 1°, AML Law).

[312] In Belgium, estate agents must be listed in the "table" (register) maintained by the IPI in order to practise legally. This register is a list of approved estate agents, both natural and legal persons, who have been licensed to practise after satisfying the legal conditions.

> ***Weighting and conclusion*** – The supervisory authorities have the necessary powers to monitor compliance and impose sanctions. Shortcomings are observed in the monitoring of persons with a significant or controlling interest and beneficial owners in certain DNFBPs (C.28.4 b). For newly covered company service providers, the limitations set out in C. 22.1 apply. **Belgium is largely compliant with R.28.**

Recommendation 29 – Financial Intelligence Units (FIU)[313]

R.29 has been reassessed as the 2017 AML Law includes provisions relating to the Belgian FIU: the Financial Intelligence Processing Unit (Cellule de Traitement des Informations Financières – CTIF) Belgium was rated compliant in the 2015 MER.

Criterion 29.1 – The CTIF is the central authority responsible for receiving, processing and transmitting information relating to the AML/CFT and for analysing information received in connection with AML/CFT (Art. 76 and 79 AML Law). The CTIF disseminates the results of its analyses to the various competent authorities (judicial, customs, tax administration, supervisory authorities, etc.) (Art. 82 and 83 AML Law).

Criterion 29.2 – The CTIF is the central agency for receiving reports from obliged entities, including suspicious transaction reports (STRs) (Art. 79 § 1 AML Law). In addition to STRs, which are linked to subjective criteria of suspicion, the CTIF receives and processes other communications drawn up on the basis of objective criteria, notably: reports of non-compliance with the ban on cash payments for immovable property (Art. 66 § 2, para. 3 AML Law), and cross-border cash transportation declarations (RD of 26 January 2014 and EU Regulation 2018/1672).

Criterion 29.3 –

a) The CTIF may, if necessary, request additional information (of a financial, administrative or judicial nature) from the reporting entities, beyond that contained in the initial reports (Art. 48 and Art. 81§1 AML Law).

b) The CTIF may also request any information of a financial, administrative or law enforcement nature that is deemed useful for the performance of its duties (Art. 81§1 AML Law). The CTIF may question and obtain information from the supervisory authorities (notably the BNB and the FSMA – the main supervisory authorities of FIs, see R.28, as well as SPF Economy), the President of the Bar (under certain conditions provided for in Art. 52 of the AML Law, see c23.2 a), bankruptcy receivers and interim administrators, judicial authorities, State administrative services, public social action centres and police services. The collection of information from the public authorities is facilitated by the secondment of liaison officers to the CTIF. Through the liaison officers of the federal police, the CTIF can obtain information from the public prosecutor's database (ADBA) and the police database. With regard to administrative services, the CTIF can question the federal services as well as certain regional and community services, such as the Flemish tax administration (which assumed responsibility for collecting and paying inheritance tax in 2015). It can also access the SPF Finance tax databases directly. The CTIF can also exchange information with the Anti-Fraud Coordination Service, which reports to the General Administrator of the Special Tax Directorate (in charge of combating tax fraud) and with the General Customs and Excise Administration, among others.

With regard to TF, the Law of 29 March 2024 creates the common database (BDC TER)[314] to centralise personal data and information relating to the prevention and monitoring of terrorism and extremism likely

[313] R.29 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its mutual evaluation in 2015

[314] The joint "Terrorism, Extremism and Radicalisation Processes" database enables the sharing of unclassified information on the following six categories of people in real time: foreign terrorist combatants, home-grown terrorist combatants, potentially violent extremists, hate mongers and convicted terrorists.

to lead to terrorism. The CTIF can access this data bank (Art. 4. § 1 of the Royal Decree of 14 July 2024) and populate this database according to strategic, tactical or operational needs.

Criterion 29.4 – Article 76 §3 of the AML Law describes the CTIF's analysis function as including the analysis of reports to identify specific targets and the analysis of trends to improve detection.

(a) Operational analysis – This focuses on reports to identify specific targets, track suspicious activities or operations and establish links with crimes, ML /TF or PF. CTIF's Money Laundering and Terrorist Financing Department conducts operational analyses based on the information it receives and collects.

(b) Typological and strategic analysis – The Strategic Analysis Department (created in 2009) is responsible for conducting proactive research into ML/TPF trends, designed to reinforce operational analysis. In particular, it has recently examined ML linked to Chinese criminal circles, corruption, drug trafficking, virtual currencies, corporate structures, and Italian- and Albanian-speaking organised crime groups. Since 2023, it has published a twice-yearly newsletter entitled "RADAR", which analyses confirmed trends and weak signals.

Criterion 29.5 – The AML Law allows the CTIF to disseminate, spontaneously or on request, the results of its analyses and useful information to the competent authorities concerned.

Competent judicial authorities:

- Spontaneously: to the judicial authority (public prosecutor or federal prosecutor, Art. 82 § 2, para. 1) and to the European Public Prosecutor's Office (Art. 24 Regulation (EU) 2017/1939) as soon as a serious indication of ML/TF is identified.
- Upon request: the public prosecution service, investigating judges, the police acting on a warrant, or the Central Unit for Seizure and Confiscation (OCSC) (Art. 84 § 1, Art. 4, para. 1, 50°).
- When CTIF transmits a file to the public prosecutor's office, it spontaneously shares all relevant information with the other competent AML/CFT authorities, such as the supervisory authorities (BNB, FSMA, SPF Economy), SPF Finance, Customs and the agencies combating social security fraud (Art. 83 § 2 AML Law).

Cooperation with other entities (spontaneously and upon request): Foreign FIUs (Art. 83, § 2, 1°; Art. 122-124 AML Law) (see R40); European Anti-Fraud Office (OLAF): (Art. 83, § 2, 2° AML Law and Art. 8.3 of Regulation No 883/2013); Supervisory Authorities (Art. 83, § 2, 3°; Art. 121 § 2) and Treasury (Art. 83, § 2, 6°); Intelligence Services (Art. 83, § 2, 4°); the OCSC (Art. 82 § 2, para. 2 AML Law).

The CTIF only spontaneously transmits information that may be useful for the performance of the duties of other competent authorities for AML/CFT matters, including SPF Finance, the European Anti-Fraud Office (OLAF), the supervisory authorities (notably the BNB, the FSMA and SPF Economy) and the intelligence authorities (Article 83 § 2).

Although Article 84 of the AML law authorises dissemination upon request, the law does not specify the technical details of the channels used. However, the CTIF has signed several memoranda of cooperation (MOUs) with bodies such as OLAF, BNB and FSMA. These memoranda set out the practical procedures for exchanging information, specifying the use of secure systems and e-mail, while ensuring the protection of confidential data, according to the urgency of the situation. This information is transmitted to the State Security services via a liaison officer. However, transmissions to the judicial authorities are still made in paper format and physically submitted (for the main public prosecutor's office in the Kingdom (Brussels), by post or by e-mail). Since October 2024, CTIF has been using the secure goAML platform for all exchanges with reporting entities.

The CTIF may, spontaneously and upon request, share information and analyses with other FIUs via secure channels such as FIU.net and Egmont Secure Web (Art. 122 to 126 AML Law).

Criterion 29.6 –

(a) A comprehensive system has been put in place to guarantee the confidentiality of the information held by the CTIF and its dissemination in accordance with the provisions of the AML Law (Art. 83 § 1, Art. 58 and Art. 65 § 3, para. 5). The CTIF has drawn up memos[315] for all employees, which are incorporated into the labour regulations and cover document security, IT security policy and the ethical framework (professional secrecy, loyalty, conflicts of interest, abuses of power).

(b) CTIF staff are subject a reinforced professional secrecy requirement, prohibiting any external communication regarding the existence and content of individual files (Art. 83, § 1 AML Law), with the penalties set forth in Art. 458 of the Belgian Criminal Code. Memos and a code of ethics govern several aspects of the protection of sensitive and confidential information. An internal security officer oversees the application of these provisions, including the security of premises and documents, and the prevention of conflicts of interest and abuses of power

(c) The CTIF has drawn up memoranda concerning the security of premises and IT security policy.

Criterion 29.7 –The CTIF is an administrative authority with a separate legal personality from that of the State (Art. 76 AML Law), which enables it to have its own assets, the right to perform all acts necessary to achieve its purpose, and legal representation. The following elements ensure its independence and operational autonomy:

(a) *Power to exercise its functions freely* – the CTIF has extensive autonomy, both in the exercise of its mission (decisions to be taken, external collaboration, internal organisation, etc.) and at the administrative level (including for its budget). The arrangements for the composition, organisation, operation and independence of the CTIF are determined by the Royal Decree of 20 March 2022. The CTIF can thus make independent decisions about the assignment of its staff, including the hiring of new members of staff and internal promotions. With the exception of a few liaison officers, it does not work with seconded personnel.

(b) *Exchange of information*: The CTIF has adequate powers to conclude agreements or decide independently to collaborate with other national competent authorities or with its foreign counterparts via memoranda of understanding (Art. 76 §2 AML Law).

(c) *Governance*: The CTIF is under the joint administrative control of the Ministers of Justice and Finance, who have no control over the CTIF's decision-making powers. It is independent and autonomous in the analysis and transmission of data, without receiving instructions (Art. 76 § 2).

The CTIF is headed by a President appointed by the King, on the proposal of the Minister of Justice (Art. 71 § 1 AML Law and Art. 2 of the Royal Decree of 20 March 2022). As with all CTIF members, the President is appointed following a selection process, and conditions of appointment must be met, which ensure that the successful candidate has the necessary expertise and experience to hold this key position. This appointment is made at the recommendation of the College of Prosecutors General, following a call for applications from Belgian judges who meet the criteria of expertise and experience set out in the AML Law.

The CTIF's governance also includes a Bureau, consisting of the President, the Vice-President and a Secretary General responsible for the day-to-day management of the CTIF's activities (Art. 4 RD 2022). The CTIF itself recruits its permanent secretariat, including the heads of department.

(d) *Use of resources* – although the Ministers for Justice and Finance determine the maximum amount of the CTIF's budget, the CTIF draws up its own budget, which it manages independently. Its budget is not borne by the State but consists of contributions paid annually by entities subject to the AML law (exception granted to lawyers, linked to the exercise of the rights of defence).

[315] Memo No 1: Terms of enhanced professional secrecy; Memo No 2: Security of premises; Memo No 3: Document security ("Clean desk policy"); Memo No 4: Ethical framework (loyalty to the CTIF); Memo No 5: Abuse and misuse of power; Memo No 6: Conflicts of interest, management of gifts and benefits.

Criterion 29.8 –The CTIF is one of the founding members of the Egmont Group.

> *Weighting and conclusion* – Dissemination upon request is provided for by law, but the lack of clarity regarding the technical modalities constitutes a minor deficiency. **Belgium is largely compliant with R.29**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities[316]

Recommendation 30 has been reassessed to take account of the introduction at European level of the European Public Prosecutor's Office (EPPO) by Regulation 2017/1939. Belgium was rated compliant with R.30 in the 2015 Mutual Evaluation Report.

Criterion 30.1 – In Belgium, several prosecution authorities are able to conduct investigations into CB, FT or ML predicate offences. The Minister of Justice is responsible for judicial investigations carried out under the orders of local prosecution authorities and the Federal Prosecutor. Responsibility for investigating and prosecuting ML offences is shared between the public prosecutors' offices within the judicial districts (ECOFIN section). The distribution of ML cases between judicial districts is based on various criteria (geographical criteria, international or organised crime dimension, etc., and with regard to the Belgian Code of Criminal Procedure (*Code d'instruction criminelle* – CIC)). The Federal Public Prosecutor's Office has subsidiary jurisdiction over criminal prosecutions and takes action on its own initiative. The magistrates within the Labour Inspectorates (*Auditorats du travail*) are responsible for cases of social security fraud linked to ML. The public prosecutor may decide to refer complex cases to an investigating judge. The Federal Public Prosecutor's Office prosecutes a limited list of offences (including TF) and endeavours to facilitate international cooperation.

The two levels of police (local and federal) are autonomous but operate in an integrated and complementary manner. The Federal Police Criminal Investigation Department (*Police Judiciaire Fédérale* – PJF) carries out specialised and supra-local judicial policing missions throughout the country, while also supporting local police forces and other police authorities. It is placed under the authority of the Ministers for the Interior and Justice, who can issue the orders, instructions and directives necessary for its criminal investigation missions. Within the Directorate General of the Police Criminal Investigation Department (*Direction Générale de la Police judiciaire fédérale* – DGJ), the 14 decentralised criminal investigation departments ("PJF") are responsible for conducting ML and TF investigations.

At the EU level, the European Public Prosecutor's Office (EPPO) was established by EU Regulation 2017/1939. Belgium participates in the EPPO and the EPPO investigates and prosecutes offences affecting the financial interests of the European Union, such as fraud (see EU Directive 2017/1371 for a list of offences), as well as any other criminal offence that is inextricably linked to criminal conduct that falls within the scope. All EU member states are required to criminalise the listed offences, which include money laundering involving property derived from the criminal offences listed in EU Directive 2017/1371.

In addition to investigative powers that are available to EPPO prosecutors under their respective national law, certain investigative measures and other measures are available to the EPPO under Art. 30 (1) of EU Regulation 2017/1939, provided that the offence under investigation carries a maximum penalty of at least four years of imprisonment. These include the power to track and trace objects, search and seizure, order the production of objects, documents or computer data, freeze instrumentalities or proceeds of crime and intercept electronic communications.

[316] R.30 has been reassessed because of the changes to the legal, regulatory or operational framework applicable in Belgium since the 2015 MER and the 2018 FUR.

Criterion 30.2 – Investigators in the PJF conducting investigations into the ML predicate offence are permitted to conduct a parallel financial investigation. In TF matters, the dedicated terrorism research agencies within the PJFs not only carry out specific investigations into TF, but also handle the financial aspect as part of broader investigations into terrorist cases. One or more investigating judges specialising in terrorism cases are appointed within the jurisdiction of each court of appeal.

Criterion 30.3 – The prosecuting authorities have the power to identify, trace and initiate proceedings for the seizure of property likely to be the proceeds of crime (see R.4). Asset investigations may be ordered by the public prosecutor or investigating judge in order to assess the assets to be seized. The public prosecutor's office may also request that the trial judge, after a conviction, carry out a specific investigation of material benefits (*enquête pénale d'exécution* – EPE). In 2022, the DGJ adopted an internal directive creating a specialised "assets" team (PLUK) within each PJF, responsible for systematically incorporating the financial and asset dimensions into investigations. The Law of 4 February 2018 strengthened the OCSC's role in asset investigations. The Customs Administration has the power to withhold certain funds as part of controls on the cross-border transportation of cash (see R.32).

Criterion 30.4 – The authorities empowered to conduct financial investigations into predicate offences are prosecuting authorities as described in Criterion 30.1. In addition, the Special Tax Inspectorate (ISI) within SPF Finance is responsible for combating certain financial offences, including serious tax fraud, financial swindling and misappropriation of corporate assets. Joint investigation teams (MOTEM), bringing together investigators from the DGJ and tax or social security experts, may be formed up in ML matters (circular COL 02/2023 of the College of Prosecutors General). The Customs Administration also contributes to combating fraud, organised crime and terrorism and to implementing obligations relating to the control of the cross-border transportation of funds (see R.32).

Criterion 30.5 – In Belgium, ML/TF investigations and prosecutions resulting from or related to the offence of corruption are generally carried out by the federal authorities.

Weighting and conclusion – **Belgium is compliant with R.30.**

Recommendation 31 – Responsibilities of law enforcement and investigative authorities[317]

R.31 has been reassessed as Belgium has made changes to its legal framework with the entry into force of the Law of 8 July 2018 organising a central contact point for financial accounts and contracts.[318] Belgium was deemed compliant with the requirements of R.31 in the 2015 MER.

Criterion 31.1 – During investigations of ML, predicate offences and TF, the police use traditional investigative methods (exploitation of open sources, seizures, hearings, searches, etc.) as provided for in the Belgian Code of Criminal Investigation (CIC).

(a) The production of documents held by IFs, DNFBPs (Art. 46 *quater* para. 4, CIC). Persons subject to professional secrecy (including notaries, accountants and tax advisers) may voluntarily hand over the documents requested or, failing that, a targeted search may be carried out on the orders of the investigating judge, who is responsible for deciding which documents are covered by professional secrecy and therefore may not be seized (Art. 458 of the Criminal Code). A special regime applies to lawyers, who may never

[317] R.31 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its mutual evaluation in 2015.

[318] Law of 8 July 2018 on the organisation of a central contact point for financial accounts and contracts and extending access to the central file of seizure, delegation, assignment, collective debt settlement and protest notices, and its implementing orders.

voluntarily hand over documents covered by professional secrecy to the public prosecutor or an investigating judge, nor testify in court (Art. 458 quarter CP).

Regarding the participation in the EPPO, please cf. R.30. Regarding the participation in Europol, please cf. c. 40.1.

(b) Searches of premises: officers in the police criminal investigation department may search private premises (home or business premises) under a search warrant issued by an investigating judge (Art. 46 *quinquies* and 89 *bis* CIC). Searches are only possible if the judicial authorities have compelling evidence that an offence has been committed and if other means of investigation do not appear to be sufficient to establish the truth (Art. 46 *quinquies* CIC).

(c) Gathering of evidence as part of the judicial investigation (Art. 47 *bis* CIC). Persons subject to professional secrecy may not be interviewed but may give evidence in court (Art. 458 of the Belgian Criminal Code – CP).

(d) Seizure and gathering of evidence: the public prosecutor or examining magistrate may seize anything that can be used to establish the truth (Art. 35 CIC). All evidence must be obtained fairly and lawfully (Art. 28 *bis* CIC).

The Special Tax Inspectorate (*Inspection Spéciale des Impôts* – ISI) uses the prerogatives of the Belgian Income Tax Code (*Code des impôts sur le revenu* – CIR) and the VAT Code to conduct its investigations, particularly into tax fraud, and to gain access to any document or information it deems necessary, including access to business or other premises and the production of documents held by financial institutions under certain conditions (Art. 315 to 321 CIR).

In addition to their investigative powers at national level, the prosecutors at the European Public Prosecutor's Office, in which Belgium participates, also have investigative powers relevant to the implementation of R.31 to investigate and prosecute the perpetrators of money laundering offences harming the financial interests of the European Union. These include the power to locate and trace objects, search and seize, order the production of objects, documents or computer data, freeze instruments or proceeds of crime and intercept electronic communications (Art. 30 (1) of Regulation (EC) No 2017/1939 of the Council).

Criterion 31.2 – In the context of a judicial inquiry or investigation, the police criminal investigation department police may use the following investigative methods under the supervision of the public prosecutor or investigating judge:

- undercover operations (deferred intervention including monitored deliveries (Art. 40 *bis* CIC), infiltration, observation, use of informers (Art. 47 *ter* to 47 *undecies* CIC);
- interception of communications and telecommunications (Art. 90 *ter* CIC on intercepting, taking cognisance of, examining and recording communications not accessible to the public or data from a computer system);
- access to computer systems (Art. 39 *bis*; Art. 90 *ter* and Art./ 88 *ter* CIC). The ISI may gain access to the IT systems of the natural or legal persons it inspects (Art. 315 *bis* CIR).
- Monitored delivery: the Law of 6 January 2003 on special investigation methods and certain other investigation methods governs the interception of mail, discreet visual checks and delayed interventions (including monitored deliveries, see above). The Law of 4 February 2010 on methods of data collection by the intelligence and security services provides the latter with other search methods relevant to AML/CFT.

Criterion 31.3 –

(a) Belgium has reinforced mechanisms that enable it to identify, in a timely manner, whether natural or legal persons hold or control accounts. The Law of 8 July 2018 (Art. 6) grants authorised persons (including the CTIF (Art. 81.§1 AML Law), judicial authorities (Art. 46 *quater*, § 2 CIC), the police and the Central Unit for

Seizure and Confiscation (OCSC) (Art. 22, § 1 Law of 4 February 2018)) direct access to the Central Point of Contact (PCC) register of financial accounts and contracts held by the National Bank of Belgium. The PCC centralises information on financial accounts and contracts opened in Belgium. All banking, foreign exchange, credit, savings, insurance, lending and electronic money institutions are required to transmit information and data relating to the accounts and contracts of a financial nature that they hold, any changes made to them and the existence of financial transactions involving cash (Art. 3, 4 and 7). The data recorded in the PCC is kept for a period of 10 years (Art. 20). Persons registered in the PCC register are not informed of requests for information made in the context of detection, investigation and prosecution in criminal matters (Art. 8).

(b) The public prosecutor's office may have direct access to information from the PCC and may also request information from banking institutions by means of a written, justified decision (Article 46 *quater* para. 3, CIC). This information is obtained without prior notification of the owner (Art. 46 *quater* para. 3, CIC).

Criterion 31.4 – The police can only access information held by the CTIF if it has first been forwarded to the public prosecutor, notably via the Federal Police liaison officers seconded to the CTIF. Nonetheless, this general rule can be legally waived. Art. 81 §2 of the AML Law stipulates that police services may spontaneously transmit information about ongoing investigations to the CTIF. If the CTIF has information that is useful to investigators and if there are serious indications of ML or TF within the meaning of the law (which, according to the authorities, applies when the investigation concerns one of the predicate offences referred to in the law), the CTIF will transmit the information in its possession to the judicial authorities and will inform the investigators of this transmission.

The judicial authorities (i.e. public prosecutors, investigating judges, police and the OCSC – Art. 4 50° AML Law) may ask the CTIF to obtain all of the relevant information it holds, and send it reasoned requests for financial information and financial analyses when such information or financial analyses are necessary in the case of an investigation (Art. 84 AML Law and Art. 21 Law of 4 February 2018). The CTIF may also spontaneously pass on information to magistrates and investigators (Art. 81§1 and 82 §2 AML law)

Weighting and conclusion – Belgium is compliant with R.31.

Recommendation 32 – Cash couriers[319]

R.32 has been reassessed because the European framework for cash movements has changed since the 2015 MER. Regulation 1889/2005 of 26 October 2005 of the European Parliament and of the Council on controls of cash entering or leaving the European Community has been replaced by Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls of cash entering or leaving the Union. Belgium also amended the Royal Decree of 26 January 2014 (RD 2014)[320] in August 2021 to take account of the provisions of the new European Regulation. Belgium was rated compliant with the requirements of R.32 in the 2015 Mutual Evaluation.

Criteria 32.1 – Article 3 of EU Regulation 2018/1672 requires natural persons entering or leaving the EU to declare accompanied cash (defined, inter alia, to include any currency and bearer negotiable instruments (BNIs)), to the value of EUR 10 000 or more. This applies if the cash is on the traveller's person, in their luggage or in their means of transport. Article 4 of the Regulation provides that where unaccompanied cash (including by post, courier, unaccompanied luggage or containerised cargo) of EUR 10 000 or more is entering or leaving the Union, the competent authorities (defined as customs and any other authorised

[319] R.32 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its mutual evaluation in 2015.

[320] Royal Decree of 26 January 2014, laying down certain measures relating to controls on the cross-border transportation of cash.

authorities) may require the sender or recipient (or an authorised representative) to make a disclosure declaration within a deadline of 30 days.

Belgium has supplemented the European system and applies a control regime on demand to movements of cash into or out of an EU Member State based on the provisions of the RD of 26 January 2014, as amended in August 2021.

Criterion 32.2 – Article 3 of EU Regulation 2018/1672 requires a written declaration for all travellers carrying cash to the value of EUR 10 000 or more, using a template declaration form as laid out in Commission Implementing Regulation (EU) 2021/776. Art 3 also states that "The obligation to declare cash shall not be deemed to be fulfilled if the information provided is incorrect or incomplete or if the cash is not made available for control" i.e. an obligation that the declaration is truthful.

Belgium has introduced a written or electronic declaration system for the incoming and outgoing cross-border transportation of cash or BNIs between Belgium and non-EU third countries above the threshold of EUR 10,000 or equivalent value (Art. 2 Royal Decree 2014). The obligation includes a requirement for the declaration to be true (Art. 3 Regulation (EU) 2018/1672).

Criterion 32.3 – Belgium applies a system for the communication, upon request, of incoming and outgoing funds between Belgium and EU Member States above the threshold of EUR 10,000 (Art. 4 Royal Decree 2014) as well as for unaccompanied cash inbound from and outbound to non-EU States (Art. 4 Regulation (EU) 2018/1672). The information must be appropriate and provided in good faith (Art. 6 RD 2014). For unaccompanied cash, the obligation includes providing the authorities with appropriate and truthful information upon request (Art. 4 Regulation (EU) 2018/1672).

At the EU level, for unaccompanied cash, Art. 4 of EU Regulation 2018/1672 provides that "The obligation to disclose unaccompanied cash shall not be deemed to be fulfilled where the declaration is not made before the deadline expires, the information provided is incorrect or incomplete, or the cash is not made available for control" i.e. to provide authorities with appropriate and truthful information upon request.

Criterion 32.4 – At the EU level, see c.32.2 and 32.3 above. EU Regulation 2018/1672 allows competent authorities to temporarily detain the cash in such cases (see c.32.8), but does not provide any power to request or obtain additional information from a traveller (in the case of a false declaration) or a sender/recipient (in cases of a false disclosure declaration.

At the national level, customs and excise officers and police officers are empowered to verify compliance with the obligation to declare/communicate by inspecting individuals, their means of transport and their luggage, and to require the presentation of documents establishing the identity of the persons concerned and obtain information (via a standardised declaration form) on the origin of the sums, the owner and recipient of the sums and the use to which they are put (Art. 6 and 7 RD 2014). Information on the bearer of the sums, the transport route and the means of transportation is also requested (via the forms introduced by Regulation 2018/1672).

Criterion 32.5 – *At the EU level*, Article 14 of EU Regulation 2018/1672 requires member states to introduce effective, proportionate and dissuasive penalties for cases where there has been a failure to comply with the declaration or disclosure requirements. Thus, each member state determines the amount and nature of any sanctions, and should do so in line with Art.14.

Belgium lacks sufficiently proportionate penalties for false declarations/communications. The obligation to declare/communicate is deemed not to have been fulfilled in the event of incorrect or incomplete information, (Art. 6 of the Royal Decree of 26 January 2014, amended in 2021). Any breach or attempted breach of the obligation to declare and disclose extra-EU movements of funds (pursuant to Regulation (EU) 2018/1672) is punishable by a fine of between EUR 125 and EUR 1,250 (double in the event of a repeat offence) as part of a settlement with the customs authorities. The scale of transactional fines is set out in

Instruction 2024/I/7 and Circular 2022/C/21.[321] The amount of the fine is calculated progressively according to the amounts not declared. The maximum fine is EUR 1,250 if the amount not declared exceeds EUR 500,000. Consequently, the maximum limit set is not fully proportionate to the intentional act of not declaring such substantial amounts. With regard to intra-EU movements of funds, any breach of this obligation falls within the remit of the public prosecutor and is punishable by a prison sentence of between eight days and five years and a fine of between EUR 25 and EUR 25,000.

Criterion 32.6 – At the EU level, Article 9 of EU Regulation 2018/1672 requires that the competent authorities shall record the declaration and disclosure information and make it available to the FIU of the Member State where the information was obtained as soon as possible, and in any event within 15 days. Information is transmitted through the "Custom Information System – CIS", a database directly accessible by the FIU, in accordance with Article 5 of Implementing Regulation 2021/776. The FIU is also required to share the information with relevant FIUs from other EU member states in accordance with Article 53(1) of EU Directive2015/849. All EU member state FIUs are connected to CIS. The CTIF also has access to customs declarations attesting to non-compliance with the reporting obligations under Articles 3 and 4 of Regulation (EU) 2018/1672 and suspicious transaction reports for amounts below the EUR 10,000 threshold suspected of being linked to criminal activity (Art. 9 RD 2014).

Criterion 32.7 – Notwithstanding the requirement assessed in c.32.6, there are no EU requirements ensuring adequate coordination between relevant authorities at a national level on the implementation of R.32. Cooperation between customs agencies and the police on issues relating to the cross-border movement of funds is based on a framework agreement which organises their collaboration, exchanges of information and a joint analysis of risks and fraud, particularly in the event of joint controls. The Law of 18 March 2014 on the management of police information therefore authorises the two-way communication of data and other information to enable other authorities to carry out their statutory duties. The terms and conditions of this communication are set out in a memorandum of understanding approved by the ministers concerned in 2012. Access to information held by the immigration authorities and exchanges of such information are authorised with police authorities, but not directly with customs agencies, which do not have investigative powers.

Criterion 32.8 – Article 7 of EU Regulation 2018/1672, which has to be implemented under national law, allows competent authorities to temporarily detain cash when the obligation to declare or disclose cash has not been fulfilled or when there are indications that the cash (irrespective of the amount) is related to criminal activity. The initial detention period is limited to 30 days, but this can be extended by competent authorities to 90 days in appropriate cases, where this is necessary and proportionate.

The competent authorities are empowered to seize cash or BNIs temporarily in the event of non-compliance with the obligation to report or communicate movements of funds, where false reports or information are communicated or where there is a suspicion of ML/TF or predicate offences. However, the maximum retention period of 14 days for the movement of funds between EU Member States is insufficient (Art. 8 para. 2 and 3 RD 2014). A judicial seizure of the funds may be ordered at the end of this period to allow the funds to be held for a reasonable period in order to establish whether evidence of ML/TF is likely to be found.

Criterion 32.9 – There are no obstacles likely to hinder Belgium's ability to cooperate with the competent foreign authorities with regard to cash transfer declarations and communications.

At the EU level, Article 10 of EU Regulation 2018/1672 requires exchange of declaration/disclosure information with competent authorities in other EU member states, and Art.11 allows such exchange of such information through mutual administrative assistance with authorities in third countries (subject to

[321] Instruction 2024/I/7 on the cross-border transportation of cash issued by the General Customs Administration, and Circular 2022/C/21 on the cross-border transportation of cash, published on the Belgian Ministry of Finance website

conditions). Art.9(2) also requires exchange of such information with relevant FIUs in other EU member states. Under Art.13 all declaration/disclosure information (which includes information on the currency/BNI, and the identification data of the traveller/carrier) is to be retained for five years, and may be further retained for an additional period of up to three years in specific circumstances.

At the national level, all the information referred to in (a); (b); and (c) is stored in the Customs database (see C.32.6, Art. 9 RD 2014). The CTIF has access to this information, which enables exchanges with foreign FIUs (Art. 123-124 AML Law 2017). Belgium is also a party to the Convention of 18 December 1997 on Mutual Assistance and Cooperation between Customs Administrations (Naples II). Finally, it also implements Regulation 515/97, which aims to establish rapid and efficient exchanges of information between customs authorities. A Europe-wide customs information system contains information on movements of undeclared funds.

Criterion 32.10 – Article 13 and recital 33 require that the use of personal data shall be carried out in accordance with EU law, and compatible with the purposes of Regulation 2018/1672. Any collection, disclosure, transmission, communication and other processing of personal data is also subject to the requirements of Regulations (EC) 45/2001 and (EU) 2016/679 of the European Parliament and of the Council. Article 11 requires that any transmission of cash information to a third country is subject to the written authorisation of the competent authority which originally obtained the information and should also comply with national and EU law on the transfer of personal data to third countries.

All EU member states are part of an internal market, an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured (Art. 26/2 TFEU and Preamble of EU Regulation 1889/2005).

Criterion 32.11 – In the event of non-compliance with the obligation to communicate or if the obligation to report has been fulfilled but there are indications that the cash originates from or is intended to finance an illegal activity, the cash will be detained by the competent authority (see C.32.8). If this suspicion is confirmed, seizure and confiscation measures may be ordered by the judicial authority under the conditions described in R.4. The sanctions described in R.3 and R.5 are also available.

> ***Weighting and conclusion*** **–** Belgium lacks sufficiently proportionate penalties for false declarations or disclosures. This deficiency is particularly significant in Belgium, given the scale of flows transiting through the country and the country's risk environment, which is characterised by the predominant use of cash trafficking in ML/TF cases. The maximum retention period of 14 days for the movement of funds between EU Member States is insufficient. **Belgium is partially compliant with R.32**.

Recommendation 33 – Statistics[322]

R.33 has been reassessed because Belgium has adopted the Royal Decree of 30 November 2020, which imposes statistical obligations. Belgium was re-rated as largely compliant for this Recommendation in the 2018 Follow-up Report (partially compliant in the 2015 MER). Some of the shortcomings identified in 2015 had been remedied by the provisions requiring the keeping of statistics, which were introduced by the AML Law of 17 September 2017.

Criterion 33.1 – The Belgian authorities are required to keep comprehensive statistics, which are published annually, in order to contribute to risk assessment and to measure the effectiveness of the AML/CFT system (Art. 71 and 72 AML Law).

[322] R.33 has been reassessed at the request of Belgium which has made regulatory changes since the 2018 Follow-Up Report.

(a), **(b)** and **(c)** The statistics referred to are required by Art. 4 2° of the Royal Decree (RD) of 30 November 2020.

(d) The only statistical information required for international cooperation is that relating to the CTIF's cooperation with other FIUs (Art. 4 4° RD 30 November 2020).

> *Weighting and conclusion* – Statistics on international cooperation should be required from all the authorities concerned. **Belgium is largely compliant with R. 33**.

Recommendation 34 – Guidance and feedback[323]

R.34 has been reassessed following the adoption of new guidelines and feedback initiatives. Belgium was assessed as largely compliant in the 2015 MER. Despite progress in sectoral feedback from the supervisory authorities, the 2018 Follow-Up Report confirmed persistent failings, particularly in the absence of recent specific measures for non-financial professions (casinos, lawyers and bailiffs). The largely compliant rating was maintained.

Criterion 34.1 –

The supervisory authorities must inform reporting entities of their AML/CFT obligations, by means of circulars, recommendations or other forms of communication. They must also raise their awareness of ML/TF risks and developments in the legal framework, a requirement that also applies to the self-regulatory authorities (Art. 86 § 2 AML Law)**.**

For FIs - The regular publication of circulars by the BNB and the FSMA, in addition to guidelines by SPF Finance and Economy on the implementation of AML/CFT obligations meet the requirements of R.34 – providing FIs with useful, up-to-date guidance that is available online. The training measures for AML/CFT compliance officers (AMLCOs) organised by the FSMA and the BNB are few in number (BNB: one in 2019 and one in 2024, and two sessions by the FSMA in 2022 and 2023 respectively). However, these authorities also take part in annual round-table discussions with the private sector, during which they provide feedback to taxable persons. This limited provision could constitute a weakness with regard to R.34, which advocates practical support for the guidelines, which should help reporting entities to better understand and fulfil their AML/CFT obligations.

For non-financial sectors – The Belgian authorities disseminate guidelines for DNFBPs, notably through regular publications either intended for all obliged entities (e.g. SPF Economy), or for certain categories, especially when they are issued by supervisory authorities or self-regulatory bodies (chartered accountants, notaries, lawyers, bailiffs). SPF Finance has published various documents (circulars, handbooks, explanatory notes) to clarify the AML/CFT measures on financial sanctions, high-risk countries and beneficial owners. However, disparities persist in terms of updating and accessibility: some sectors (casinos) lack up-to-date resources, which limits their ability to respond to regulatory changes and emerging risks. For the sectors identified as having the highest ML/TF risk:

- The diamond-trading sector – SPF Economy supervises diamond dealers via a regulation (March 2024) and a guide on financial penalties. However, no TF guidelines have been issued and the quantity and quality of the documents made available has increased recently. SPF Economy has also published a compliance guide on financial sanctions specifically for diamond dealers, which supplements the Treasury's guidelines on this subject (see below) and on high-risk countries.
- For estate agents, SPF Economy published a regulation (last updated in April 2022). SPF Economy and the Belgian Professional Institute of Estate Agents (*Institut Professionnel des Agents Immobiliers*

[323] R.34 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its 2018 Follow-Up Report.

– IPI) collaborated to publish a procedures manual in 2022 that provides detailed guidelines, practical templates and AML/CFT indicators to raise estate agents' awareness of their AML/CFT obligations. However, the guidelines do not appear to be regularly updated.

In addition, awareness-raising and training initiatives are uneven. Certain initiatives, such as the articles of the French- and German-speaking bars association (*Ordre des barreaux francophones et germanophones* – OBFG) for lawyers and the FAQs for notaries, and those of the ITAA through practical tools, provide ongoing support to non-financial professions in response to ML/TF risks. However, other sectors, such as casinos, bailiffs, diamond merchants and real estate, appear to be receive less support for the application of their AML obligations from their respective supervisory authorities.

Like SPF Economy, the CTIF also supports all reporting entities by publishing educational information (covering financial sanctions, high-risk countries and asset freezing obligations), guidelines and annual reports. It also organises training seminars. Finally, it collaborates with the supervisory authorities, such as the BNB, FSMA and ITAA, notably on the reporting activities of the obliged entities under their supervision.

Feedback - Feedback is generally given in the form of annual reports, sector consultations and communications, and specific communications following inspections, such as those carried out in the insurance and payments sectors. However, FSMA's sectoral feedback remains limited. The BNB's annual report also presents a general overview of AML/CFT controls over the year, including the salient points, but provides few sector-specific details.

The CTIF also provides feedback to reporting entities in accordance with the requirements of the AML Law (Art. 78, Art. 83 and 121 §2 and §3). However, CTIF's sectoral feedback in its annual report focuses mainly on the statistics for reports submitted by sector, with little emphasis on the typologies revealed by suspicious transaction reports, which are described in general terms but not by sector.

The Belgian *AML platform*,[324] established in 2021, has also enhanced dialogue by bringing together financial institutions, regulators and the CTIF for regular discussions on practices for detecting and reporting suspicious transactions. This approach largely meets the requirements of Recommendation 34. The AML platform is currently focusing primarily on financial institutions, with non-financial professions playing little part in the discussions.

> ***Weighting and conclusion*** – The supervisory authorities, the CTIF and the self-regulatory bodies must implement measures to help financial institutions and DNFBPs understand and comply with their AML/CFT obligations. However, VASPs and certain DNFBP sectors (such as casinos) lack up-to-date documents and training, which may reduce the effectiveness of measures taken in response to changing risks and regulations. **Belgium is largely compliant with Recommendation 34.**

Recommendation 35 – Sanctions[325]

Belgium was found to be largely compliant with R.35 in the 2015 MER in the absence of established criteria for assessing the proportionality of the range of sanctions available to financial institutions, either in the specific context of AML/CFT controls or through prudential controls. For some DNFBPs, the main shortcoming was the fact that a disciplinary penalty needed to be imposed on the senior managing official before sanctions could be imposed on legal entities. R.35 was re-assessed as compliant in the 2018 Follow-Up Report.

[324] A description of this platform is included in the Introduction.

[325] 2015 Mutual Evaluation Report and Follow-up Report for Belgium (2018)

Criterion 35.1 – Articles 132 to 139 of the AML Law 2017 provide for administrative (Art. 132-135) and criminal (Art. 136-138) sanctions imposed by AML/CFT supervisory authorities, including for breaches of financial embargoes (transposition of Directive 2015/849). The scope of application is broad. The range of penalties is comprehensive and described in a hierarchical manner. The thresholds and ceilings for penalties differ for legal entities and natural persons. The criteria used to determine the nature and proportionality of the sanction are set out in Art. 132 § 3, namely:

- consideration of all relevant circumstances;
- the seriousness and duration of the offence;
- the degree of responsibility;
- the defendant's financial situation;
- the advantage and profits derived from the offence;
- any losses suffered by third parties;
- the defendant's degree of cooperation; and
- any previous offences.

The application of these criteria allows for the imposition of proportionate penalties. In the interests of prevention, administrative penalties are published, subject to certain exceptions, on the supervisory authorities' websites.

Criterion 35.2 – When a sanction is imposed on a legal entity, it is also possible to sanction natural persons, i.e. members of the legal administrative body or the management committee, as well as the persons who, in the absence of a committee, participate in the effective management of the legal entity and who are responsible for the infringement found.

> *Weighting and conclusion* – The shortcomings identified for R.35 have been remedied by the introduction of criteria for defining the nature and proportionality of sanctions in the AML/CFT Law. **Belgium is compliant with R.35.**

Recommendation 36 – International instruments[326]

Belgium was rated compliant with the requirements of R.36 in the 2015 MER.

Criterion 36.1 – Belgium is a Party to the Conventions of Vienna (since 1996), Palermo (since 2004), Mérida (United Nations Convention Against Corruption) (since 2008) and the Convention on TF (since 2004), the Council of Europe Convention on Cybercrime (since 2009) and that on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and TF (since 2010).

Criterion 36.2 – Belgium has reinforced its compliance with the provisions of the Conventions of Vienna, Palermo and the Convention on TF through the laws of 14 December 2016amending the Criminal Code with regard to the suppression of terrorism, and of 5 May 2019 notably relating to provisions on criminal matters, and has fully implemented the Merida Convention.

> *Weighting and conclusion* – **Belgium is compliant with R.36**.

[326] Mutual Evaluation Report for Belgium (2015)

Recommendation 37 – Mutual legal assistance[327]

Belgium was rated largely compliant with the requirements of R.37 in the 2015 MER. The main shortcomings concerned the lack of clear procedures for prioritising and implementing requests for mutual legal assistance. In addition, the case management system did not enable the monitoring or control of the implementation of letters rogatory. In the absence of a re-rating request, the 2018 Monitoring Report noted that the Law of 6 July 2017 on the simplification, harmonisation, computerisation and modernisation of the provisions of civil law and of the notarial profession, and on various justice-related measures has led to the introduction of a more flexible procedure for implementing foreign requests for mutual legal assistance. The Law has ended the requirement to obtain prior authorisation for the implementation of a request for mutual assistance involving search and seizure and to obtain authorisation for the transmission of evidence obtained. According to the Belgian authorities, this change will reduce the time taken to implement requests for mutual assistance. In the absence of a re-rating request, the largely compliant rating was maintained.

Criterion 37.1 – Belgium may provide mutual legal assistance to other countries on the basis of the bilateral and multilateral conventions that it has ratified, and can thus grant the broadest possible mutual legal assistance in criminal matters in accordance with the law and the applicable rules of international law (see MER 2005 for the list of treaties). The Law of 9 December 2004 on international mutual assistance in criminal matters also governs the implementation in Belgium of requests for mutual assistance from a State with which Belgium is not bound internationally by a convention on mutual assistance in criminal matters, on the basis of reciprocity.

Criterion 37.2 – SPF Justice is the central authority for international cooperation in criminal matters for requests concerning non-EU countries; requests from the EU are transmitted directly between judicial authorities and SPF Justice must be notified. Within the Public Prosecutor's Office, the Federal Prosecutor's Office is authorised to manage all types of incoming and outgoing requests for international cooperation in criminal matters. Letters rogatory drawn up in this way are transmitted either directly from judicial authority to judicial authority for countries with which Belgium is bound by an international convention, or after being authorised by the Minister of Justice in other cases.[328] The Federal Public Prosecutor's Office facilitates the implementation of requests for mutual legal assistance, irrespective of the offences in question. It is also the central contact point for judicial authorities and international institutions such as the European Judicial Network and Eurojust. The authorities state that the central authority receives a copy of each outgoing or incoming request for assistance whenever requests are made directly and that a request registration system, operational since 1st January 2004, is in place. However, the registration system does not enable the supervision or verification of the due implementation of either outgoing or incoming letters rogatory, or the measurement of the time taken for implementing the requests and cannot therefore be regarded as a management system; nor is it integrated, i.e. it cannot be accessed by the Kingdom's courts or judges. The central authority therefore does not have an automatic system for following up on letters rogatory whose implementation has been delayed, and can only react to reminders from the requesting authority. There are no formal criteria for managing request urgency or for establishing priorities and the prompt implementation of requests for mutual legal assistance. This system does not enable the collection of statistics on mutual assistance activities.

Criterion 37.3 – The grounds for rejecting requests for legal assistance in criminal matters in Belgium (aside from those in conventions) are set out in the Law of 9 December 2004. A request may be rejected if there is

[327] Follow-Up Report for Belgium (2018)

[328] Circular No COL 5/2005 from the College of Prosecutors General and the Minister for Justice contains instructions for sending and receiving requests for mutual assistance directly between judicial authorities.

no reciprocity commitment, or if its implementation could harm the sovereignty, security, public policy or other "essential interests of Belgium" (undefined, but according to the Belgian authorities this reason has never been the basis for non-implementation of a request for mutual assistance in the field of economic and financial crime). These grounds do not appear to be incompatible with those generally accepted and contained in international conventions (including conventions signed by Belgium) The authorities state that in principle, the rule is to honour requests for assistance.

Criterion 37.4 – Since the entry into force of the Law of 9 December 2004, mutual legal assistance may no longer be refused for tax offences (except as provided in conventions). A request for assistance may not be refused on the grounds of secrecy or confidentiality of financial institutions and non-financial professions, unless such information has been obtained in circumstances covered by professional secrecy. "Banking secrecy" (see C.9.1. for the definition of this concept in Belgium) is unenforceable against a judicial authority (see R.31).

Criterion 37.5 – As a general rule, bilateral conventions with Belgium provide that the requested State and the requesting State shall undertake to preserve the confidentiality of information, evidence exchanged and any action undertaken as a result of the request, or only to use the information on predefined terms. The authorities state that confidentiality is stipulated by recent mutual assistance conventions. Each request for assistance must in any event be part of a Belgian judicial file or be the subject of a new file for the purposes of its implementation. This immediately entails investigative and examining secrecy and thereby the confidentiality of the foreign request for assistance.

Criterion 37.6 – The principle of dual criminality is a condition for mutual assistance, whether or not Belgium is linked by convention to other States. However, this dual criminality does not apply to requests for mutual legal assistance for non-binding measures. Coercive measures are defined by the Belgian Code of Criminal Investigation as measures that imply a (legal) exception to fundamental rights (prosecution, seizure, arrest and preventive detention, telephone tapping and direct or indirect interception of communications, surveillance and undercover operations).

Criterion 37.7 – As the principle of dual criminality is a condition for mutual assistance, the fact that TF is not criminalised in Belgium in full compliance with the international standard may impede mutual assistance based on the requirement of dual criminality (see C.5.2)

Criterion 37.8 – The principle governing the treatment of requests for mutual assistance is that every request must be treated in the same way, using the same investigative powers as if the case had been conducted in Belgium by the Belgian authorities (see R.31).

> ***Weighting and conclusion*** – Belgium lacks clear procedures for prioritising and implementing requests for mutual legal assistance. In addition, the current case management system does not enable the monitoring or control of the implementation of letters rogatory. **Belgium is largely compliant with R.37.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation[329]

R.38 has been reassessed as Belgium has made changes to its legal framework since the 2015 mutual evaluation, with the entry into force of the Law of 4 February 2018 on the Central Unit for Seizure and Confiscation (OCSC), Regulation 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, and the amendments made to

[329] R.38 has been reassessed because Belgium has made changes to its legal, regulatory or operational framework since its mutual evaluation in 2015.

the Law of 5 August 2006 on the mutual recognition of judicial decisions in criminal matters in the EU by the Law of 28 November 2021.

Belgium was found to be largely compliant with the requirements of R.38 in the 2015 MER due to deficiencies in the criminalisation of TF that could impede mutual assistance based on the dual criminality requirement (these have since been addressed – see Belgium's 2018 Follow-Up Report and R.5 above), the impossibility of enforcing foreign confiscation orders issued without a prior conviction, and the absence of an agreement signed by the OCSC with its foreign counterparts to enable the coordination of seizure and confiscation measures.

Criterion 38.1 – Belgium has the power to implement freezing and confiscation measures in respect of the assets listed in sub-criteria a) to e), with the exception of immovable property, except in the cases exhaustively provided for in the Belgian Criminal Code (CP) (see R.4).

With regard to identification, Belgium is able to take expeditious action in response to requests for identification from EU Member States under a European Investigation Order sent directly to the competent judicial authority (the King's Prosecutor for the place in which the assets are located). The expeditious nature of the processing of requests from non-EU States in the framework of a request for mutual assistance in criminal matters addressed to the central authority (SPF Justice) is subject to minor limitations noted under R.37.

The OCSC can also provide information informally to its foreign counterparts through the CARIN networks (at international level) and the Asset Recovery Offices (AROs) (at European level) for which the OCSC has been designated as the national contact point for Belgium (Art. 30 of the OCSC Act of 4 February 2018). The OCSC must process the requests received within 14 days, with the possibility of faster processing in urgent cases (Art. 4 EU Council Framework Decision 2006/960/JHA).

With regard to freezing and confiscation

For requests issued by EU Member States: Belgium has the power to take expeditious action on the basis of Regulation (EU) 2018/1805 [330] and the Law of 5 August 2006 as amended by the Law of 28 November 2021 within the time limits set out in Articles 12 and 29 of the 2006 Law. These texts provide for the mutual recognition of freezing and confiscation orders for the items covered under (a) to (e) (Art. 2/1 7° Law of 2006). For decisions concerning criminal offences punishable by a maximum penalty of at least three years' imprisonment, listed in Article 3 of the Regulation (reflecting the offences mentioned in the FATF definition of "designated categories of offences"), the decision must be enforced without verifying the condition of dual criminality (also Art. 3 Law of 5 August 2006). In other cases, the Member State may verify the existence of dual criminality. Freezing and confiscation orders must be recognised without delay (Art. 4 para.1 law of 5 August 2006).

For requests issued by EU third countries: Belgium is able to respond expeditiously to freezing requests within the time frames set by the Law of 20 May 1997 (Chapter III). However, the expeditious processing of confiscation requests from non-EU countries is not systematically guaranteed.

Criterion 38.2 – There is no legal provision in Belgian law to enable the enforcement of foreign confiscation orders without prior conviction for non-EU countries. However, Belgium may enforce confiscation orders issued by an EU Member State in the context of criminal proceedings on the basis of European Regulation 2018/1805 and the Law of 5 August 2002 Art. 2.7). European Regulation 2018/1805 provides for the

---

[330] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders ("1805 Regulation")

recognition and enforcement of freezing orders and confiscation orders issued in the framework of criminal proceedings. Requests for the recognition of freezing orders may be issued by a judge, court, public prosecutor or other competent authority (subject to validation by a court/public prosecutor). For confiscation orders, requests may be issued by an authority that is designated as such by the issuing State and which is competent in criminal matters to enforce a confiscation order issued by a court in accordance with national law. The concept of "proceedings in criminal matters" is not defined in European Regulation 2018/1805, but the preamble specifies that it covers other types of decisions rendered without a final conviction. The regulation covers orders issued without a final conviction in criminal proceedings. It does not cover orders issued as part of civil or administrative proceedings.

Criterion 38.3 –

(a) The OCSC is the national contact point for Belgium for the CARIN networks (at international level) and the Asset Recovery Offices (AROs) (at European level) (Art. 30 of the OCSC Law of 4 February 2018). Belgium also uses Eurojust and the European Judicial Network to coordinate seizure and confiscation measures at the investigation and prosecution stages. Belgium has also signed bilateral treaties on mutual legal assistance that include specific provisions on seizure and confiscation (e.g. with the United Arab Emirates and India in 2021).

(b) Responsibility for the management of assets seized and confiscated by the Belgian judicial authorities is shared by the OCSC, the registries of the Belgian courts and SPF Finance. The same applies to the management and disposal of assets seized or confiscated in the enforcement of requests for mutual assistance from foreign authorities (Art. 7 and 31 OCSC Act 2018, and Art. 28 *octies* CIC).

Criterion 38.4 –Belgium may share confiscated assets with other countries (Art. 38 Law of 5 August 2006 and Art. 30 of Regulation 2018/1805 for EU Member States, and Art. 8 Law of 20 May 1997 in the event of cooperation with a non-EU country).

> ***Weighting and conclusion*** – Belgian law contains no legal provision for the enforcement of foreign confiscation orders without prior conviction for non-EU countries or in civil or administrative proceedings for EU Member States. There is a persistent shortcoming concerning the expeditious processing of requests for mutual legal assistance in criminal matters concerning identification and confiscation requests from authorities in EU third countries. **Belgium is largely compliant with R.38.**

Recommendation 39 – Extradition[331]

Belgium was rated largely compliant with the requirements of R.39 in the 2015 MER. The main shortcomings were the lack of a tool for prioritising and managing extradition requests, cumbersome and complex conditions for extradition outside the EU with a possible impact on deadlines, and a lack of criteria for deciding whether or not to prosecute in the event of a refusal to extradite.

Criterion 39.1 –

(a) ML and TF offences may give rise to extradition.

(b) Belgium's extradition procedures are clear but do not allow priorities to be set due to the absence of a tool for managing requests (see C.37.2). Time limits have been established at each stage of the European arrest warrant procedure under the Law of 19 December 2003. Outside the EU, conditions for implementing foreign arrest warrants remain cumbersome and complicated, with the involvement of the judge in chambers and the government (see Section 6.4, 2015 MER).

[331] Mutual Evaluation Report for Belgium (2015)

(c) The implementation of requests for extradition is not combined with unreasonable or unduly restrictive grounds or conditions. In European cases, a Member State does not enforce a European arrest warrant if (i) a final decision has already been rendered by a Member State against the same person for the same offence (ne bis in idem); (ii) the offence is covered by an amnesty in the Member State of execution; (iii) the person concerned cannot reasonably be considered responsible by the Member State of execution due to his or her age. The Law of 1874 stipulates that any extradition is dependent upon the existence of a treaty between Belgium and the requesting country. The conditions in the EU and Council of Europe treaties comply with the standard.

Criterion 39.2 – Belgium may extradite its nationals and residents in Belgian territory to an EU Member State on the basis of a European arrest warrant (if appropriate, on condition that the person concerned is returned to Belgium after conviction to serve his/her sentence). Outside the EU, Belgium does not extradite its nationals, but the Belgian authorities state that "in principle", prosecution will be undertaken if the requesting State is a party to the European Convention on Extradition or has signed a bilateral extradition agreement with Belgium. This means that Belgium can refuse to extradite its (non-EU) nationals without committing itself to prosecuting the act that gave rise to the request. The criteria for refusal are not governed by law.

Criterion 39.3 – The Law of 1874 requires that the facts giving rise to extradition are punishable both under Belgian law and under the law of the requesting State. However, it does not require the classification of the facts to be the same in the same in both countries. The Law of 19 December 2003 provides that a European arrest warrant may be enforced without verification of dual criminality in a certain number of cases including ML and TF.

Criterion 39.4 - Belgium has simplified extradition mechanisms for implementing the European arrest warrant, which therefore replace the traditional extradition system. Outside the European framework, the extradition procedure is simplified if the person concerned consents to extradition.

> ***Weighting and conclusion*** – The extradition procedures do not enable priorities to be established due to the absence of a request-management tool. In addition, the extradition conditions outside the EU are cumbersome and complicated, which does not guarantee extradition without delay The lack of criteria for deciding whether or not to prosecute in the event of an extradition refusal is also a cause for concern. **Belgium is largely compliant with R.39.**

Recommendation 40 – Other forms of international cooperation

Recommendation 40 has been reassessed to take account of provisions introduced at European level – Regulation 2016/794 on Europol and Regulation 2018/1727 on Eurojust, as well as the European Banking Authority's guidelines on cooperation and information exchange between competent authorities supervising credit and financial institutions of 16 December 2019.

Belgium was rated largely compliant with the requirements of R.40 in the 2015 MER. The identified shortcomings related to the fact that exchanges of information between non-peer authorities were not organised in Belgium. In addition, two of the supervisory authorities (SPF Economy and SPF Finance) lacked the capacity to cooperate with foreign authorities with comparable powers. R.40 was reassessed in the 2018 Monitoring Report. The rating was maintained due to persistent shortcomings concerning the lack of measures to organise information exchanges between non-counterpart authorities, with the exception of the CTIF.

Criterion 40.1 –The competent authorities in Belgium can promptly provide the widest possible range of international co-operation – both spontaneously and upon request – in the fields of ML, associated predicate offences and TF.[332] At the EU level, Belgium also cooperates in cross-border investigations and prosecutions via the European Union Agency for Criminal Justice Cooperation (Eurojust) and through cooperation in law enforcement via the European Union Agency for Law Enforcement Cooperation (Europol). Eurojust - based on EU Regulation 2018/1727 - has the tasks to support and strengthen coordination and cooperation between national investigating and prosecution authorities in relation to serious crime where that crime affects two or more member states, including in relation to money laundering activities or terrorism (Art. 3 and Annex I EU Regulation 2018/1727). Europol provides operational and strategic support to law enforcement authorities in the EU in cross-border cases of serious crime, including preventing and combating money laundering and terrorism (Art. 3 and Annex I EU Regulation 2016/794).

Criterion 40.2 –

(a) International cooperation has a legal foundation (see C.40.1).

(b) There is no impediment to use of the most effective means of co-operating (e.g. covered by Art. 122 to 128 AML Law).

(c) The CTIF and the Federal Police use clear and secure channels, circuits and mechanisms to facilitate transmission and the implementation of requests.[333]

(d) The CTIF, the Belgian General Customs and Excise Administration (*Administration générale des Douanes et Accises* –AGDA) and the Federal Police have clear procedures for establishing priorities and facilitating the transmission and timely implementation of requests (Art. 122 to 128 AML Law). There is no evidence that other competent authorities have similar communication channels and procedures.

(e) The competent authorities have clear procedures for protecting information received (see C.40.6 and Art. 64 and 65 AML Law).

At the EU level, Eurojust acts by opening a coordination case in the Case Management System that is regulated by Art. 23 EU Regulation 2018/1727 and operates based on processes and data protection standards set out by law. At the EU level, Europol has developed the Secure Information Exchange Network Application (SIENA), a state-of-the-art tool designed to enable swift, secure and user-friendly communication and exchange of operational and strategic crime-related information and intelligence between Europol, member states and Third Parties with which Europol has cooperation agreements / working arrangements. For the exchange of information, the FIU may use the system FIU.net for the exchange with FIUs of EU member states. The system is hosted by the European Commission allowing EU FIUs to securely exchange and cross-match information for the analysis of potential cases of money laundering, associated predicate offences and terrorism financing. For the exchange of information between financial supervisors, the European Banking Authority (EBA) provides the system eGATE that facilitates the exchange of information with competent authorities in EU member states supervising credit and financial institutions.

[332] CTIF: Art. 123-128 AML Law; CTIF and OLAF: Art. 83 §2 2° AML Law; CTIF and Europol: Art. 83 §2 5° AML Law; CTIF and financial sector supervisory authorities within colleges of supervisors: Art. 181/1 Banking Law (25 April 2014); Federal Police: multilateral treaties (Prüm Treaty, Convention implementing the Schengen Agreement, Interpol and Europol channels, etc.), bilateral treaties with non-EU Member States; AGDA: Regulation No 515/97, Naples II Convention and the Belgian Law on Assent of 13 September 2004; other agreements and protocols on mutual administrative assistance in customs matters with non-EU Member States; EU Council Directive on administrative cooperation in the field of taxation (2011/16/EU); Multilateral Convention on Mutual Administrative Assistance in Tax Matters as amended in 2010; double taxation avoidance treaties and agreements on exchanges of information for tax purposes; for financial sector supervisory authorities, see C. 40.12 to C. 40.16). BNB and FSMA: Art. 36/16 of the Law of 22 February 1998; Art. 77 of the Law of 2 August 2002; and Art. 131/5 et seq. of the AML law.

[333] CTIF: Art. 126 §1 AML Law, Egmont Secure Web, FIU-Net; Federal Police: Schengen Information System, EUROPOL SIENA and Interpol I24/7.

Criterion 40.3 – The CTIF, the police authorities, AGDA, the BNB and FSMA have concluded bilateral agreements, Memoranda of Understandings (MOU) and protocols to facilitate cooperation with numerous foreign counterparts. There is no indication that these agreements were not negotiated and signed in a timely manner.

Criterion 40.4 – The CTIF provides timely feedback to the competent requested authorities on the use and usefulness of information obtained (see C.40.10 and Art. 83 § 2 and 3 AML Law). Concerning the BNB and the FSMA, feedback to the requested authorities is provided systematically (either under bilateral cooperation agreements or in accordance with the provisions of European law). The Federal Police claims to provide feedback on its terrorist financing investigations upon request (without any specific legal obligation). AGDA provides feedback on the use and usefulness of the information obtained (upon request in the case of spontaneous exchanges) on the basis of the cited legal instruments governing international mutual assistance, whether administrative or criminal (e.g. Regulation 515/97, Naples II Convention); feedback is also given when the information provided discloses the commission of offences.

Criterion 40.5 – Belgium does not prohibit exchanges of information or mutual assistance with regard to the four points of this criterion, and there are no unreasonable or unduly restrictive conditions placed on them. [334]

Criterion 40.6 – Unless prior authorisation has been granted, the competent authorities have established monitoring and protective measures to ensure that exchanged information is only used for the purposes and by the authorities for which the information was sought or provided. [335]

Criterion 40.7 – The competent authorities are obliged to ensure a level of confidentiality appropriate to any request for co-operation and the information exchanged, in compliance with obligations of privacy and data protection. [336]

Criterion 40.8 – The competent authorities are able to make requests on behalf of foreign counterparts and exchange any information with them which could be obtained if such requests were made internally. [337] Requests for information sent to the CTIF by foreign FIUs are treated as suspicious transaction reports (STRs). The CTIF can therefore use all the prerogatives of the AML Law to process these declarations.

Criterion 40.9 – The CTIF has an appropriate legal basis to cooperate with its foreign counterparts in cases of ML, predicate offences and TF (see c.40.1 and c.40.2). The CTIF also actively participates in spontaneous exchanges of information.

Criterion 40.10 – If so requested, the CTIF completes and returns a "feedback statement" in respect of information provided by foreign FIUs. Moreover, the CTIF states that whenever it uses foreign information as part of a transmission to the Belgian judicial authorities (with the permission of the FIU which provided it), it systematically advises its foreign counterpart of such transmission.

---

[334] Federal Police: Convention implementing the Schengen Agreement, Articles 39 to 46; AGDA: Art. 19, Naples II Convention; BNB: Art. 36/14 Law of 22 February 1998 and Art. 130 §4 AMLA Law; FSMA: Art. 77 §2 Law of 2 August 2002 and Art. 130, §4 AMLA Law; CTIF: Art. 122, 125 to 128 AMLA Law.

[335] CTIF: Art. 458 CP; Federal Police: Art. 44, Law of 5 August 1992; Art. 83 §1, 122, 123 and 125 AML Law; Art. 458 CP; AGDA: Art. 34 et seq., Regulation 515/97; BNB: Art. 36/17 §1 3° Law of 22 February 1998; Art. 131 - 131/4 of the AML/CFT Law 2017; FSMA: Art. 75 §2, Law of 2 August 2002; Art. 131 - 131/4 of the AML Law 2017.

[336] CTIF: Art. 123, 125 and 126 AML Law, Art. 458 Criminal Code; Federal Police: circulars COL 1/2016 and MFO-3; Art. 458 Criminal Code; AGDA: Art. 320 of the General Law on Customs and Excise; BNB and FSMA: Art. 36/17, §1, 3°, and §4, Law of 22 February 1998; Art. 77 *bis*, §1, b), 3°, §5, Law of 2 August 2002; and Art. 131/5 et seq. AML Law 2017.

[337] CTIF: Art. 79 § 3 and 4, 123 § 3, 124 §2, 127, 130§1, 131/1§1, 131/3 §1 AML Law; Federal Police: MFO-3 Joint Directive of the Ministers for Justice and the Interior; AGDA: Regulation No 515/97 and Art. 8 of the Naples II Convention; BNB: Art. 36/17, Law of 22 February 1998; FSMA: Art, 77 *bis*, Law of 2 August 2002

Criterion 40.11 - The CTIF has the power to exchange all information in accordance with **(a)** and **(b)** (Art. 79, 123 to 128 AML Law).

Criteria 40.12 to 40.16 – Art. 129 to 131 of the AML Law govern cooperation between the supervisory authorities (including SPF Economy and SPF Finance) and their foreign counterparts with comparable powers (see also C. 40.8 and the specific provisions for the BNB and the FSMA[338]). These provisions enable the supervisory authorities to cooperate and exchange a wide range of information with a view to strengthening their supervisory tasks. The exchange and cooperation activities relate mainly to regulatory and prudential information and information on AML/CFT policies; they also concern the supervision of Belgian reporting entities that are branches or subsidiaries of obliged entities in another State.

At the EU level, competent authorities supervising credit and financial institutions (see c. 40.15) concluded an agreement on the exchange of information with the European Central Bank acting as a prudential supervisor. Information exchange can extend to prudential and AML/CFT information, including material weaknesses int the AML/CFT governance, systems and controls framework. For supervisors in the EU, the AML/CFT Colleges Guideline4 create a common framework to support effective oversight of cross-border groups from an AML/CFT perspective and also from a more general prudential perspective. Specifically, AML/CFT colleges provide a permanent structure for cooperation and information exchange between supervisors from different member states and third countries that are responsible for the AML/CFT supervision of the same firm. The guidelines set out the rules that govern the establishment and operation of these colleges, and structure the exchange of information between AML/CFT and prudential supervisors, who will be invited to participate in AML/CFT colleges as observers. See c. 40.2.

Criterion 40.17 – The Federal Police services are able to exchange domestically accessible information with their foreign counterparts for intelligence or investigative purposes in the context of ML, related predicate offences or TF cases, including for the purpose of identifying and tracing the proceeds and instruments of the crime (see c. 40.2 and c. 40.3). Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identifying proceeds from, or other property related to, crime provides for prompt exchanges of information enabling effective measures to combat cross-border organised crime.

Criterion 40.18 – This police co-operation takes place particularly within the legal framework of conventions signed by Interpol, Europol or Eurojust with third-party countries. At the EU level, a number of systems and databases can be used by the competent authorities of Belgium to access data in line with the established access right:

- Schengen Information System (SIS), used to enter and consult alerts on wanted or missing persons and objects.
- Eurodac, a database of fingerprints of asylum applicants registered in the EU and third-country nationals who crossed an external border illegally.
- Entry/Exit system, used to record entry and exit of third-country nationals crossing the borders of the Schengen Area. The System will also record refusals of entry.
- European Criminal Records Information System (ECRIS-TRN), used to exchange information on criminal convictions.

These data accesses on a cross-border basis complement exchanges of information with individual law enforcement authorities in EU member states and in other EU cooperation fora.

Criterion 40.19 – Joint investigation teams (JITs) are provided for in the Law of 9 December 2004 on international mutual legal assistance in criminal matters, which transposes into Belgian law the provisions of

[338] BNB: Art. 36/16, Law of 22 February 1998; FSMA: Art. 77, Law of 2 August 2002. Certain sector-specific laws also contain relevant provisions (insurance intermediaries, portfolio management and investment advice companies, collective investment undertaking management companies).

the Council Law of 29 May 2000 establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams. In a customs context, the joint special investigation team is one of the specific forms of cross-border cooperation covered by Title IV of the Naples II Convention.

Criterion 40.20 – The CTIF has the power to cooperate with non-peer authorities (Art. 127 AML Law). The AML Law also organises the international cooperation of AML/CFT supervisory authorities with certain non-counterparts (supervisory authorities (Art. 131/1 and 131/2), authorities responsible for the supervision of financial markets (Art. 131/3 and 131/4) and the European Banking Authority (Art. 131/5)). The police are also required to organise cooperation with non-police authorities through formal mechanisms (applicable provisions not available). There are no provisions applicable to the international cooperation of other AML/CFT competent authorities with non-counterpart authorities, with the exception of the Public Prosecutor's Office in TF matters, through the CTIF (Art. 79 §3 2° and 4° AML Law).

> *Weighting and conclusion* – The Belgian authorities possess extensive powers for international cooperation, but exchanges of information between non-peer authorities are not organised for all the competent authorities. **Belgium is largely compliant with R.40.**

Annex B. Technical compliance shortcomings

The Recommendations presented in green have been subject to a full assessment, reflecting either amendments to the FATF Standards or substantive changes made by the country to its legal, regulatory, or operational frameworks since its last mutual evaluation. The remaining Recommendations are based on pre-existing information from the country's most recent assessments and have not been reassessed in this review.

Recommendations	Rating*	Factor(s) underlying the rating
1) Assessing risks & applying a risk-based approach	LC	• Inadequate information mechanism on the results of national risk analyses. • Lack of a legislative framework requiring the identification, assessment and mitigation of PF-related risks.
2) National cooperation and coordination	PC	• Need to clarify the scope of responsibilities for defining national CFT and CPF policy. • Lack of representation of all the competent authorities in the CFT and CPF coordination body. • Lack of a specific framework for cooperation in CPF measures.
3) Money laundering offence	LC	• Sanctions against legal persons for ML are not sufficiently proportionate.
4) Confiscation and provisional measures	LC	• Confiscation of immovable property constituting instruments of the crime set forth in the Belgian Criminal Code provided for certain predicate offences only.
5) Terrorist financing offence	C	• All criteria are met.
6) Targeted financial sanctions related to terrorism and terrorist financing	PC	• Criteria limiting the identification of potential targets under UNSCRs 1267/1989, 1988 and 1373 to persons or entities subject to criminal proceedings. • Lack of a mechanism enabling Belgium to ask another country to give effect to freezing actions initiated at Belgian level • No legal basis for designation on the national list based on requests from a third country.
7) Targeted financial sanctions related to proliferation	LC	• Possible delays in the announcement of UN designations via the consolidated national list of TFS. • No explicit obligation to report attempted transactions to SPF Finance • Provision of targeted instructions on PF TFS.
8) Non-profit organisations	PC	• The authorities have not provided a sufficiently precise identification of which subset of organisations meets the definition of NPOs at risk of TF. • Surveillance measures do not target the TF risk. • Supervision is mainly of a general nature (governance, transparency and tax compliance) and does not specifically target terrorist financing risks. • Penalties are not calibrated or applied in line with the TF risk. Some may be disproportionate. • There is no formal organisational framework for cooperation, coordination and exchanges of information between all authorities holding relevant information on NPOs. • No point of contact or procedure has been defined for responses to international requests for information.
9) Financial institutions secrecy laws	C	• All criteria are met.
10) Customer due diligence	C	• All criteria are met.
11) Record-keeping	LC	• No legal provision setting a deadline for transmitting due diligence information to the competent authorities.

Recommendations	Rating*	Factor(s) underlying the rating
12) Politically exposed persons	C	• All criteria are met.
13) Correspondent banking	PC	• No application of the specific due diligence measures in R.13 to cross-border correspondent banking relationships within the EEA.
14) Money or value transfer services	C	• All criteria are met.
15) New technologies	NC	• Lack of a comprehensive and current legal framework for the oversight of VASPs, with particular regard to their registration, supervision and due diligence obligations. • Failure to transpose the key provisions of the MiCA Regulation and European AML Directives into Belgian law.
16) Wire transfers	LC	• No obligation for cross-border transfers up to EUR/USD 1,000, in accordance with the EU Regulation. • No obligation for the beneficiary's FI to check the accuracy of the information for transfers of EUR 1,000, except in the case of suspected ML/TF, transfers in cash or anonymous electronic money. • No explicit obligation requiring payment service providers to file a suspicious transaction report in all countries concerned by a wire transfer.
17) Reliance on third parties	LC	• Existence of an exemption scheme enabling the use of third-party introducers established in the EEA, which are not considered as third countries, despite the ban targeting high-risk countries.
18) Internal controls and foreign branches and subsidiaries	LC	• The independent audit function is not clearly defined for small FIs. The level of flexibility allowed does not maintain a minimum supervision mechanism, which may create blind spots in the supervision. • The intra-group consistency requirement remains non-binding; it is based solely on an explanatory statement with no clear legal force.
19) Higher-risk countries	C	• All criteria are met.
20) Reporting of suspicious transactions	LC	• No clear or indicative framework governing the timeframe for STR reporting to the CTIF. •
21) Tipping-off and confidentiality	C	• All criteria are met.
22) DNFBPs: customer due diligence	LC	• The shortcomings raised under R.11, 12, 15 and 17 are also applicable to R.22.
23) DNFBPs: other measures	LC	• The limitations identified under R.18 concerning the implementation of group policies abroad also apply to DNFBPs. • No obligation to report attempted transactions not carried out by lawyers.
24) Transparency and beneficial ownership of legal persons	PC	• Insufficient measures to ensure the application of the requirements of R.24 to foreign legal persons posing ML/TF risks and possessing sufficient links with Belgium. • Embryonic analysis of ML/TF risks posed by foreign legal entities linked to Belgium. • Lack of involvement of prosecution authorities in the cross-sector risk assessment of legal entities • Inadequacy of measures taken to reduce the vulnerability of legal persons to ML/TF since the reform of the Belgian Code of Companies and Associations (CSA). • Lack of a mechanism for verifying the accuracy of basic information for legal persons created by private deed. • Insufficient arrangements to prevent the misuse of shares registered in the name of nominees or directors acting on behalf of another person. • Other shortcomings linked to the international cooperation framework.
25) Transparency and beneficial ownership of legal arrangements	LC	• Insufficiently detailed analysis of the ML/TF risks associated with trusts and legal arrangements. • No obligation to hold basic information on other regulated agents and service providers of a trust or similar legal arrangement. • Other shortcomings relating to the lack of sanctions for failure to make the information referred to in R.25 available to the competent authorities.
26) Regulation and supervision of financial institutions	C	• All criteria are met.
27) Powers of supervisors	C	• All criteria are met.
28) Regulation and supervision of DNFBPs	LC	• Shortcomings identified in the supervision of persons exercising control or holding a significant interest in certain DNFBPs • No comprehensive provisions for company service providers, as the limits of

Recommendations	Rating*	Factor(s) underlying the rating
		criterion 22.1 apply to them.
29) Financial intelligence units	LC	• Lack of legal precision on the technical details of the information dissemination channels.
30) Responsibilities of law enforcement and investigative authorities	C	• All criteria are met.
31) Powers of law enforcement and investigative authorities	C	• All criteria are met.
32) Cash couriers	PC	• Penalties for false reporting or failure to report are not proportionate. • The maximum period for the temporary detention of funds for intra-EU movements is insufficient to achieve the objective of detecting ML/TF.
33) Statistics	LC	• No obligations for all competent authorities to keep statistics on international cooperation.
34) Guidance and feedback	LC	• Lack of sufficiently up-to-date information documents and lack of targeted training for certain DNFBP sectors • Limited provision of practical training and support, particularly for DNFBPs • Lack of updated or specific guidance on TF for certain high-risk sectors.
35) Sanctions	C	• All criteria are met.
36) International instruments	C	• All criteria are met.
37) Mutual legal assistance	LC	• Lack of clear procedures for prioritising and implementing requests for mutual legal assistance in a timely manner. • Inadequate system for managing requests for mutual legal assistance
38) Mutual legal assistance: freezing and confiscation	LC	• Lack of a legal basis to enable the enforcement of non-conviction-based confiscation orders without prior conviction for non-EU countries. • Expeditious processing of confiscation requests from non-EU states is not systematic.
39) Extradition	LC	• Lack of a tool for managing and prioritising extradition requests. • Terms of extradition outside the EU may lead to delays in the enforcement of foreign arrest warrants. • No obligation to prosecute its nationals if their extradition outside the EU is refused on grounds of their nationality
40) Other forms of international cooperation	LC	• Insufficient provisions to enable all competent authorities to exchange information with non-peer authorities. .

*Note: LC= Largely compliant; C = Compliant; PC=Partially compliant; NC=Non-compliant

Glossary of acronyms

Acronyms	Definitions
NRA	National Risk Analysis
SRA	Sectoral Risk Analysis
AGDA	*Administration générale des douanes et accises* (Customs & Excise)
AISBL	*Association internationale sans but lucratif* (International non-profit association)
ASBL	*Association sans but lucratif* (Non-profit organisation)
ARO	EU Asset Recovery Office Platform
ML	Money laundering
ML/TF	Money laundering/ terrorist financing
BDC	*Banque de données communes* (Joint Data Bank)
BO	Beneficial owner
BNB	*Banque nationale de Belgique* (National Bank of Belgium)
C.	Criterion
CAF	Anti-Fraud Unit of SPF Finance
CIC	*Code d'instruction criminelle* (Criminal Instruction Code)
CIR	*Code des impôts sur les revenus* (Income Tax Code)
CJH	*Commission des Jeux de Hasard* (Gaming Commission)
CNS	*Conseil national de sécurité* (National security council)
CP	*Code pénal* (Penal Code)
CPC	*Code de procédure criminelle* (Criminal Procedure Code)
FIU	Financial Intelligence Unit
CSR	*Collège de supervision des réviseurs* (Audit Oversight Board)
CSA	*Code des sociétés et des associations* (Companies and Associations Code)
CTIF	*Cellule de traitement des informations financières* (Belgian FIU)
DGJ	*Direction Générale de la Police Judiciaire Fédérale* (Directorate General of the Federal Police Criminal Investigation Department)
DJSoc	*Direction de la lutte contre les criminalités graves et organisées* (Serious and Organised Crime Division – Federal Police Criminal Investigation Department)
STR	Suspicious transaction report
CI	Credit institution
EEA	European Economic Area
EMI	Electronic money institution
PI	Payment institution
EPE	*Enquête pénale d'exécution* (enforcement investigation in criminal cases)
DNFBPs	Designated non-financial businesses and professions
EPPO	European Public Prosecutor's Office
FEDNOT	Belgian Federation of Notaries
PF	Financing of the proliferation of weapons of mass destruction
FSMA	Financial Services and Markets Authority
TF	Terrorist financing
FATF	Financial Action Task Force
FI	Financial institution

BNI	Bearer negotiable instrument
IPI	*Institut Professionnel des Agents Immobiliers* (Professional Institute of Real Estate Agents)
IRE	*Institut des Réviseurs d'Entreprises* (Institute of Statutory Auditors)
ITAA	Institute for Tax Advisors and Accountants
ISI	*Inspection Spéciale des Impôts* (Special Tax Inspectorate)
Justban	Central register of disqualifications from management
JIC	*Joint Intelligence Centre*
JDC	*Joint Decision Centre*
AML/CFT/CPF	Anti-money laundering, countering the financing of terrorism and countering the financing of the proliferation of weapons of mass destruction
MOTEM	Joint multi-disciplinary investigation teams
MoU	Memorandum of understanding
SRB	Self-regulatory body
NPOs	Non-profit organisation
OCAM	*Organe de coordination pour l'analyse de la menace* (Threat Analysis Coordination Body)
OCSC	*Organe central pour la saisie et la confiscation* (Central Office for Seizure and Confiscation)
OLAF	European Anti-Fraud Office
PCC	Central register for financial accounts and contracts
GDP	Gross domestic product
PJF	*Police Judiciaire Fédérale* (Federal Police Criminal Investigation Department)
PEP	Politically exposed person
VASPs	Virtual asset service provider
CSP	Company service provider *(centres d'affaires* – "business centres"*)*
R.	Recommendation
UNSCR	United Nations Security Council Resolution
MER	Mutual Evaluation Report
IO	Immediate outcome
SA	*Société anonyme* (public limited company)
SGRS	*Service général du renseignement et de la sécurité* (General Intelligence and Security Service)
SIC	*Société d'investissement en créances* (debt investment company)
SNC	*Société en nom collectif* (general partnership)
SPF	Service public fédéral (Federal Public Service)
SRL	*Société à responsabilité limitée* (limited-liability company)
TBML	*Trade-Based Money Laundering*
TRIM	*Target, Recup, Impact, Mode criteria*
EU	European Union
VSSE	Belgian State Security Service

www.fatf-gafi.org

December 2025

Mutual Evaluation of Belgium - Anti-money laundering and countering the financing of terrorism and proliferation financing measures

In this report: a summary of the anti-money laundering (AML)/countering the financing of terrorism (CFT)/counter-proliferation financing (CPF) measures in place in Belgium at the time of the on-site visit between January-February 2025.

The report analyses the level of effectiveness of Belgium's AML/CFT/CPF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.