

FATF



Anti-money laundering and counter-terrorist financing measures

Belgium

Mutual Evaluation Report

April 2015





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 the website: 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.

Citing reference:

FATF (2015), *Anti-money laundering and counter-terrorist financing measures -Belgium*, Fourth Round Mutual Evaluation Report, FATF.
www.fatf-gafi.org/topics/mutualevaluations/documents/mer-belgium-2015.html

© 2015 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photocredits coverphoto: ©Thinkstock

Contents

EXECUTIVE SUMMARY.....	5
A. Key Findings.....	5
B. Risks and General Situation	7
C. Overall Level of Compliance and Effectiveness	7
D. Priority Actions	9
Table 1. Effective Implementation of Immediate Outcomes	10
Table 2. Compliance with FATF Recommendations.....	16
MUTUAL EVALUATION REPORT OF BELGIUM.....	25
Preface	25
1. ML/TF RISKS AND CONTEXT.....	27
1.1 ML/TF Risks	27
1.2 Materiality.....	28
1.3 Structural Elements.....	29
1.4 Other Contextual Factors.....	29
1.5 Scoping of Issues of Increased Focus	30
2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION	33
2.1 Background and Context	34
2.2 Technical Compliance (R 1, R 2, R 33).....	36
2.3 Effectiveness: Immediate Outcome 1 (Risk, Policy and Co-ordination)	37
2.4 Recommendations on National AML/CFT Policies and Co-ordination.....	42
3. LEGAL SYSTEM AND OPERATIONAL ISSUES	45
3.1 Background and Context	47
3.2 Technical Compliance (R.3, R.4, R.29-32)	47
3.3 Effectiveness: Immediate Outcome 6 (Financial Intelligence).....	48
3.4 Effectiveness: Immediate Outcome 7 (ML Investigation and Prosecution)	55
3.5 Effectiveness: Immediate Outcome 8 (Confiscation)	63
3.6 Recommendations on legal system and operational issues.....	69
4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION	71
4.1 Context.....	72
4.2 Technical compliance (R 5 – R 8)	72
4.3 Effectiveness: Immediate Outcome 9 (TF Investigation and Prosecution).....	73
4.4 Effectiveness: Immediate Outcome 10 (Preventive Measures and Financial Sanctions relating to TF)	76
4.5 Effectiveness: Immediate Outcome 11 (TFS relating to PF).....	77
4.6 Recommendations on terrorist financing and proliferation financing.....	79
5. PREVENTIVE MEASURES.....	81
5.1 Background and Context	83
5.2 Technical compliance (R 9 to R 23).....	88
5.3 Effectiveness: Immediate Outcome 4 (Preventive Measures).....	91
5.4 Recommendations on Preventive Measures.....	101
6. SUPERVISION	105
6.1 Background and Context	107

6.2	Technical Compliance (R 26 – R 28, R 34, R 35)	108
6.3	Effectiveness: Immediate Outcome 3 (Supervision)	109
6.4	Recommendations on supervision	122
7.	LEGAL PERSONS AND ARRANGEMENTS.....	125
7.1	Background and Context	126
7.2	Technical Compliance (R 24, R 25).....	129
7.3	Effectiveness: Immediate Outcome 5 (Legal Persons and Arrangements)	130
7.4	Recommendations on Legal Persons and Arrangements	136
8.	INTERNATIONAL CO-OPERATION	139
8.1	Background and Context	140
8.2	Technical Compliance (R 36 – R 40)	140
8.3	Effectiveness: Immediate Outcome 2 (International Co-operation)	141
8.4	Recommendations on International Co-operation	144
	TECHNICAL COMPLIANCE ANNEX.....	145
1.	INTRODUCTION.....	145
2.	AML/CFT POLICIES AND CO-ORDINATION	147
	Recommendation 1 – Assessing risks & applying a risk-based approach	147
	Recommendation 2 – National co-operation and co-ordination.....	149
	Recommendation 33 – Statistics	149
3.	LEGAL SYSTEM AND OPERATIONAL MATTERS.....	151
	Recommendation 3 – Money laundering offence	151
	Recommendation 4 – Confiscation and provisional measures.....	152
	Operational and prosecutorial matters	153
	Recommendation 29 – Financial Intelligence Units.....	153
	Recommendation 30 – Responsibilities of law enforcement and investigative authorities.....	154
	Recommendation 31 – Powers of criminal prosecution and investigative authorities.....	155
	Recommendation 32 – Cash couriers	156
4.	TERRORISM FINANCING AND PROLIFERATION FINANCING.....	159
	Recommendation 5 – Terrorist financing offence	159
	Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing.....	161
	Recommendation 7 – Targeted financial sanctions related to proliferation.....	166
	Recommendation 8 – Non-profit organisations (NPOs)	168
5.	PREVENTIVE MEASURES.....	171
	Recommendation 9 – Financial institution secrecy laws.....	171
	Customer Due Diligence and Record-Keeping	171
	Recommendation 10 – Customer Due Diligence.....	171
	Recommendation 11 – Record-keeping.....	174
	Additional measures in the case of specific customers and activities	175
	Recommendation 12 – Politically exposed persons (PEP)	175
	Recommendation 13 – Correspondent banking.....	176
	Recommendation 14 – Money or value transfer services	177
	Recommendation 15 – New technologies.....	179
	Recommendation 16 – Wire transfers	179
	Reliance on third parties, Controls and Financial Groups.....	182
	Recommendation 17 – Reliance on third parties.....	182
	Recommendation 18 – Internal controls and foreign branches and subsidiaries	183

Recommendation 19 – Higher-risk countries	184
Reporting of Suspicious Transactions.....	185
Recommendation 20 – Reporting of suspicious transactions.....	185
Recommendation 21 – Tipping-off and confidentiality	186
Designated non-financial Businesses and Professions.....	186
Recommendation 22 – DNFBPs: Customer due diligence	186
Recommendation 23 – DNFBPs: other measures.....	187
6. SUPERVISION	189
Recommendation 26 – Regulation and supervision of financial institutions.....	189
Recommendation 27 – Powers of supervisors	191
Recommendation 28 – Regulation and supervision of DNFBPs.....	191
Recommendation 34 – Guidance and feedback	193
Recommendation 35 – Sanctions	194
7. LEGAL PERSONS AND ARRANGEMENTS.....	195
Recommendation 24 – Transparency and beneficial owners of legal persons	195
Recommendation 25 – Transparency and beneficial owners of legal arrangements	198
8. INTERNATIONAL CO-OPERATION	201
Recommendation 36 – International instruments.....	201
Recommendation 37 – Mutual legal assistance.....	201
Recommendation 38 – Mutual legal assistance: freezing and confiscation	202
Recommendation 39 - Extradition	204
Recommendation 40 – Autres formes de coopération internationale	205
TABLE OF ACRONYMS.....	209

Executive Summary

1. This report provides a summary of the anti-money laundering (AML) / counter-terrorist financing (CFT) measures in place in Belgium as at the date of the on-site visit (30 June to 15 July 2014). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Belgium's AML/CFT system, and provides recommendations on how the system could be strengthened.¹

A. Key Findings

- Belgium's **legal framework** for AML/CFT needs to be brought into line with the FATF requirements as revised in 2012.
- **Belgium conducts a large part of its AML/CFT activities and initiatives on the basis of risk.** However, its understanding of these risks is fragmented and incomplete. The recent national ML and TF assessments provide a useful basis for full and ongoing understanding of these risks even though not all parties concerned contributed directly to this work. **An overall AML/CFT approach still needs to be put together, based on prioritising risks and allocating resources** (for example in the judicial area and in implementing controls).
- The **financial intelligence unit (CTIF)** collects and analyses quality data on ML/TF activity and suspicious transactions. The CTIF needs to work more closely with the AML/CFT supervisors and the businesses and professions covered by the system, particularly in addressing the identified risks, and with the criminal prosecution authorities to help pool and enhance knowledge and analyses.
- The **financial sector** has a good understanding of the risks and generally seems to take appropriate preventive measures, including in high risk situations. However, tighter risk-based AML/CFT controls are needed to ensure that these obligations are being adequately applied.

1 This evaluation was prepared on the basis of the 2013 FATF Methodology. This means it is substantially different in nature from previous assessments. It includes the new obligations introduced in the 2012 revision of the FATF Recommendations, and therefore the technical compliance assessment is not directly comparable to the previous evaluation. It also assesses the effectiveness of Belgium's AML/CFT system on the basis of the new effectiveness methodology, which takes a fundamentally different approach to the technical compliance assessment. It sets out conclusions on how well the AML/CFT measures are working in practice, based on comprehensive analysis of the extent to which the country achieves a defined set of outcomes that are central to a robust AML/CFT system. Both qualitative and quantitative information are used to support that analysis.

- Inadequate understanding and implementation of AML/CFT measures was noted for some money value transfer service (**MVTS**) providers, particularly those operating via a network of agents in Belgium, and certain **bureaux de change**, which represent substantial money laundering (ML) / terrorist financing (TF) risks due the use of cash for their transactions. In addition, the suspicious transaction reporting policy applied by some of these services is not adequate. From this perspective there are shortcomings in the controls in place for these institutions.
- Improvements were seen in the **non-financial sector's** commitment to AML/CFT. However, not all designated non-financial businesses and professions (DNFBPs) concerned have taken action, including a number of at-risk professions such as lawyers and casinos.
- The implementation of AML/CFT measures by diamond dealers does not seem adequate to guarantee control of the sector's high risks. Supervision of these players remains extremely limited, notably due to a lack of available resources. Despite the proven risk of money being laundered into this sector, suspicious transaction reports (STRs) are totally lacking. The number of investigations and prosecutions seems insufficient up to now given the identified level of risk, even though two significant cases are currently under investigation.
- Actions to verify compliance with restrictions on payments in cash are carried out on target activities at risk for ML/TF, such as the trade in used cars or gold. They have already led some professionals to change their practices, but more resources are needed in this area.

B. Risks and General Situation

2. Belgium has taken an approach based on risks in its AML/CFT activities and initiatives for many years. Nevertheless, its understanding of these risks is fragmented and incomplete. Belgium conducted its first national and general ML and TF risk assessments in 2013-2014. This body of work provides a useful and encouraging basis for full and ongoing understanding of these risks, although the identified risks still need to be prioritised.

3. Based on generally available information, it appears that the activities exposed to high ML risk include the **diamond** trade, in which Antwerp is a leading world centre, and sectors in which **cash** circulates, such as the trade in used cars and gold. **Money transfer** services are also particularly exposed to ML risk in this context. The geographic position of Belgium also makes it a target for the transit of illegal movements of funds. Identifying some of these risks has already given rise to preventive and law enforcement actions (with regard to the circulation of cash, for example), but a real overall AML approach still needs to be defined.

4. In terms of terrorist financing, the main risks at present concern activities relating to **'jihadists'** travelling to countries in the Near and Middle East. Recent events in these regions and the continuing radicalisation in segments of the population create undeniable risk. The **money transfer** sector is particularly vulnerable to these threats.

C. Overall Level of Compliance and Effectiveness

5. Belgium has the basic core elements needed to develop a solid AML/CFT regime. The legal framework technically complies in broad terms but still needs to be adapted to the revised FATF requirements of 2012. As to effectiveness, Belgium has achieved substantial results in international co-operation, use of financial information and prosecution of terrorist financing acts. Only moderate improvements are needed in these areas. Major improvements need to be made in other areas:

C.1 Belgium has conducted a national assessment of its ML and TF risks but needs to incorporate the findings into its national AML/CFT policy

6. A large part of the existing AML/CFT measures in Belgium are based on its understanding of risk. The framework for assessing ML/TF risks and the mechanisms for co-operation and co-ordination at the national level were recently institutionalised. Two risk assessments were developed for ML and TF. The result provides a good basis for the overall and ongoing understanding of these risks; however, this understanding does not appear to be exhaustive at this stage, and limitations were observed, particularly in terms of the input contributed. At the time of the on-site visit, the authorities still needed to ensure that the non-confidential results of both analyses were disseminated to the concerned entities (only the professional associations had received the ML risk assessment), develop an overall AML/CFT approach and allocate resources according to the risks identified. In terms of co-ordination among the various players, improvements could be made to ensure that expertise and intelligence developed by all competent parties can be fully exploited.

C.2 Prosecution of ML needs to be more targeted

7. Belgian law enforcement agencies do treat ML as an offence: it is frequently prosecuted, notably in connection with economic offences that generate substantial profits because it facilitates confiscation of these funds (fraud, offences related to bankruptcy, benefit fraud and tax fraud). Belgium is also a leader in confiscating property when its legal origin cannot be established, in which case the person can be convicted for ML without being convicted for the predicate offence that generated the funds.

8. It is rarer however that cases reveal structured ML systems involving third parties who offer their assistance in laundering proceeds from the offences. The financial intelligence unit (FIU) and law enforcement authorities are competent and have all of the necessary investigative measures at their disposal; however, limited resources prevent them from pursuing all of the possible financial ramifications. Moreover, better co-ordination among authorities could also help identify connections between operating methods found in seemingly unrelated cases.

9. A large number of laundering cases are also linked to financial crime – such as tax fraud – and involve more structured and sophisticated laundering, notably with misuse of offshore structures. In cases such as these, international mutual legal assistance is necessary but not always successful.

10. Developing a national AML strategy that addresses the risks identified and takes stock of the situation (for which statistics would be useful) would help define targets for investigations and thus produce more effective results.

C.3 Combatting terrorist financing that is discrete but effective

11. While assessment of the country's TF risks is not yet complete, the authorities responsible for preventing and combatting terrorism and TF are well-co-ordinated and aware of the current risks, particularly with regard to individuals and small groups travelling to conflict areas. Some TF convictions have been handed down and international co-operation in this area is very well-developed, especially with neighbouring countries that face the same risks.

12. However, certain investigative programmes carried out in the past could be repeated (such as closer monitoring of certain non-profit organisations [NPOs]), and Belgian authorities should consider using targeted financial sanctions to prevent terrorists and terrorist organisations from financing their activities. Finally, the authorities should resolve the technical problems that keep them from applying targeted financial sanctions without delay when designations occur (this comment also applies with regard to the financing of proliferation of weapons of mass destruction).

C.4 The financial sector appears to apply preventive measures satisfactorily, but non-financial businesses and professions need to improve in this area

13. The financial institutions interviewed seem generally to have a good understanding of the ML/TF risks and to apply appropriate AML/CFT measures according to those risks, including stronger measures when risk is higher. However, risk-based AML/CFT controls need to be strengthened to ensure that these obligations are being adequately applied.

14. Certain of the non-financial sectors have made efforts to raise ML/TF awareness among professionals, but other sectors are still downplaying their exposure to these risks, particularly diamond dealers and casinos. In general, DNFBPs seem to apply basic due diligence measures but less so enhanced measures.

15. Belgium is confronted with a high volume of STRs, which are not based on suspicions of ML/TF. A large proportion come from the bureau de change and funds transfer sectors and consist of (automatic) STRs submitted systematically defensively by the reporting entities in the absence of any suspicion for any new transactions carried out by a customer for whom an STR has already been made. These reports should be distinguished from follow-up STRs, which are useful. Furthermore, DNFBPs that are required to submit STRs on the basis of thresholds or criteria often prefer this type of reporting and do not attempt to make an evaluation of suspicion. Other sectors, however, such as lawyers and diamond dealers, submit almost no STRs. These practices have been continuous for several years; measures are needed both to improve the quality of suspicious transaction reporting policy applicable to reporting entities and thus to enhance the detection and prosecution of acts of ML/TF.

C.5 ML/TF risk-based controls need to be implemented for all entities subject to the obligations

16. In the financial sector, inspections are implemented according to the institutions' prudential risks, but inspection priorities are not sufficiently determined by the ML/TF issue. As a general rule, there are not enough specific and qualitative on-site inspections to verify compliance with AML/CFT obligations. This is of particular concern for vulnerable sectors such as money transfer services, especially those provided in Belgium by agents of a European payment institution that is a leader in the sector. The National Bank of Belgium (BNB) recently established a framework for remote inspection that takes ML/TF risks into account.

17. In general, AML/CFT supervision of DNFBPs remains extremely limited or inexistent, even in high risk sectors (e.g. diamond dealers or lawyers). ML/TF risks are not taken into account in particular when determining the scope of supervision operations.

18. For the financial and non-financial sectors, the limited controls, the significant lack of sanctions applied solely in ML/TF matters, and the lack of resources for conducting controls seriously impair the effectiveness of AML/CFT measures.

19. Recent actions to verify compliance with restrictions on payments in cash were aimed at sectors that are particularly exposed to ML/TF risks (trade in used cars and gold) and have already had a positive impact on professional practices, which could be further improved if more resources were allocated to these controls.

C.6 Measures underway to improve the transparency of legal persons and better evaluate their exposure to ML/TF risks.

20. The competent authorities have identified several concrete risks and other vulnerabilities in the framework that governs legal persons and are taking measures to make these entities more transparent in order to prevent their misuse. As such, the AML/CFT regime should be applied promptly to domiciliation companies.

21. The competent authorities have access to basic information along with information on beneficial ownership for the large majority of legal persons. This information is available through public registers. The fact that notaries must authenticate instruments relating to the creation and existence of the large majority of legal persons reinforces the information source. However, it is regrettable that the registers are not always kept up-to-date. Initiatives are underway to eliminate these updating problems, which appear to be widespread.

22. Information available in the registers mainly indicates the company's legal ownership, which may coincide with its beneficial ownership. Other means exist to help determine beneficial ownership, such as information obtained by financial institutions and non-financial professions, or any publicly available information on publicly and non-publicly traded Belgian companies.

D. Priority Actions

- Based on the national risk assessments, competent authorities should **set priorities in terms of ML/TF actions and recommendations** and relay them to the policy makers for use in defining a national AML/CFT policy covering everything from prevention to suppression of ML and TF.
- In particular, **the lack of resources in the Belgian judicial system**, which exists in varying degrees at every level, directly impairs the detection, prosecution and sanctioning of complex ML. A concrete and co-ordinated strategy for the criminal prosecution of ML is needed.
- All of the AML/CFT control authorities should **establish a supervision based on ML/TF risks** by adapting the scope, frequency and intensity of supervision according to the nature of the risks. On-site inspections that adequately correspond to the risks also need to be implemented. Appropriate resources should be allocated to supervision based on the nature and level of ML/TF risks facing the various sectors.
- The competent authorities should **emphasise dialogue and communication with the entities concerned** on the ML/TF obligations applicable to them, what is required of them in terms of STRs and the results of AML/CFT supervisory actions.

Table 1. Effective Implementation of Immediate Outcomes

Effectiveness	
1. Risk, Policy and Coordination	Substantial
<p>Belgium evaluates its ML and TF risks. It appears to understand TF risks correctly and to have taken co-ordinated action at the national level to attenuate those risks. This co-ordination includes as well the combatting of proliferation financing. While the risks of ML appear to have been generally identified and understood, the analysis of this activity does not appear to be based on a proactive approach that would enable the detection of trends and emerging phenomena, notably with regard to vulnerabilities. In particular, the assessments did not have the participation of all competent authorities or the private sector.</p> <p>Elements of a risk-based approach have long contributed to AML/CFT policies and activities in Belgium. The CTIF and to a large degree the criminal prosecution authorities (the police in particular) have an established tradition of taking the identified risks into account when defining their objectives and activities. Nevertheless, certain weaknesses were noted at the time of the on-site visit:</p> <ol style="list-style-type: none"> i. there is no overall, integrated approach that adequately ranks ML/TF risks in order to ensure the organisation and consistent planning of AML/CFT activities and policies; ii. supervisors and self-regulatory bodies (SRBs) have not incorporated the main ML/TF risks into their inspection policies; iii. a certain number of identified ML risks have not been addressed; and iv. incomplete dissemination of the non-confidential results of the risk assessments to financial institutions and DNFBPs slows down their being taken into account in their internal procedures. 	
2. International Cooperation	Substantial
<p>Belgium's partners find the international co-operation it provides to be of good quality. No countries reported any major difficulties with Belgium's information exchange practices, and the assessors did not see any indication of serious ineffectiveness in the handling of international co-operation by the Belgian system. The interviews with the various competent authorities confirmed this finding, which was particularly positive in the area of combating TF and terrorism. In practice, the legal limitations that were found do not appear to have a major impact on the exchange of information.</p>	
3. Supervision	Moderate
<p>In the financial sector, supervisors have generally identified the main high risks. However, the understanding of the risks is too irregular due to insufficient controls, particularly on-site inspections. At present, the BNB mainly conducts its controls on a prudential basis, and the implementation of ML/TF risk-based controls is limited. On-site inspections are also limited, due to underestimation of the ML/TF risks faced by the institutions and lack of resources. The shortcomings in terms of supervision are of particular concern for financial institutions operating in Belgium under the European Passport, operating under freedom of establishment via agents</p>	

Effectiveness

in Belgium. The BNB recently began using a periodic questionnaire, which will provide it with specific and systematic information on ML/TF risks and allow it to set supervision priorities more effectively.

The AML/CFT controls implemented by the Financial Services and Markets Authority (FSMA) target the *bureau de change* sector, identified as the sector exposed to the greatest ML/TF risk; they are appropriate. Nevertheless, this control should be reinforced with regard to STR quality due to the large proportion of automatic STRs. For collective investment fund management companies, investment management and investment advisory companies and mortgage credit services, given the more limited risks these activities present, AML/CFT controls are included in the more general on-site inspections. For the financial intermediary sector, no other specific and qualitative on-site inspections are in place to verify compliance with AML/CFT obligations. A tightening of controls is thus necessary.

Federal Public Service (FPS) Finance has conducted on-site inspections at Bpost, for information only, on the AML/CFT systems and procedures in place, but no on-site inspection operation has been conducted to date. For the financial sectors under the supervision of FPS Economy, no inspections have been conducted. However, these are low-risk sectors (mortgage and direct financing lease providers).

The main supervisors of the financial sector have an active policy to promote understanding of ML/TF risks and explain AML/CFT obligations, primarily through a concrete and detailed Guidance and joint circulars (BNB/FSMA), and referral to the website and annual report of the CTIF.

The DNFBP supervisors have been designated and the regulatory systems are in place. In general, the highest risks have been identified by these authorities, but systems still need to be set up for ensuring that these risks are known and understood and for monitoring how they change over time. In general, supervision of DNFBPs remains extremely limited or inexistent. When there is a risk-based approach, it is limited to the assessment included in the annual AML/CFT report; this determines the priorities in terms of businesses to inspect. However, there is no differentiation in the subsequent controls carried out, which are uniform.

For the financial and non-financial sectors, there needs to be greater co-operation between the supervisors and the CTIF, particularly in improving the policy for all reporting entities. Limited controls and significant lack of sanctions applied, specifically in ML/TF matters, have a major impact on the effectiveness of AML/CFT measures.

FPS Economy conducts targeted supervision operations to verify compliance with restrictions on payments in cash, and ML/TF risk is one of the elements considered in selecting the target sectors. As these controls have only recently been introduced, the results are difficult to measure, but they have already prompted some professionals to change their practices. Greater resources need to be allocated to these inspections so that large-scale operations can be conducted.

4. Preventive Measures

Moderate

Financial institutions seem to have a good understanding of the risks. It appears that not all DNFBPs understand the degree of risks to which they are exposed or the need to protect themselves against potential ML/TF-related abuse.

Effectiveness

AML/CFT obligations are generally well-understood by financial institutions, and AML/CFT measures implemented are proportionate and appropriate with regard to the corresponding risks. However, shortcomings were found among some payment institutions and *bureaux de change*, particularly inadequate understanding of the requirements relating to beneficial ownership and politically exposed persons (PEPs). The financial sector also appears to apply enhanced due diligence measures in situation recognised as 'high risk', but less so for correspondent banking and wire transfers within the EU.

In recent years, many DNFBPs have made efforts to raise awareness and motivate professionals with regard to AML/CFT. These types of operations need to continue so that satisfactory implementation of the measures can be achieved. The enhanced measures applied by DNFBPs, for example, seems insufficient for situations requiring increased attention. When customer due diligence (CDD) requirements cannot be met, DNFBPs indicate that they refuse to enter into a business relationship or perform the transaction, even if they do not issue an STR. The implementation of AML/CFT measures by diamond dealers does not seem adequate to address the sector's high risks.

As a general rule, the financial sector has adopted the practice of issuing STRs, but some *bureaux de change* and payment institutions operating via a network of agents also submit a significant share of automatic STRs, which do not provide additional information on the transactions of a customer who has already been reported. DNFBPs reporting transactions on the basis of thresholds / criteria prefer this type of 'objective' reporting and do not reflect the level of suspicion raised by the related transactions. Lawyers and diamond dealers submit almost no STRs. This approach can hinder the detection of ML and contribute to under-prosecution of certain offences.

The competent authorities need to strengthen their AML/CFT controls in order to verify that the entities subject to the obligations are adequately applying them.

5. Legal Persons and Arrangements

Moderate

Authorities' understanding of the vulnerabilities with regard to legal persons remains sector-based, and is not drawn from an overall, up-to-date and continuing assessment. The criminal prosecution authorities specialised in counter-terrorism are aware of the risks of legal persons being misused for TF purposes. Depending on the case, the authorities monitor these risks on a continuing basis although they have not done a recent assessment of such risks.

Competent authorities have identified concrete ML/TF risks and vulnerabilities in the framework for legal persons. Several initiatives have been taken to address these; however, the recent implementation of certain of these measures at the time of the on-site visit, and the need for more time to fully appreciate their impact, mean that they cannot yet be considered fully effective. The authorities are aware that additional measures need to be taken.

Basic information and information on beneficial ownership for the large majority of legal persons are publicly available through the information maintained in the companies register – *Banque-Carrefour des Entreprises* (BCE) – although there are shortcomings, in particular regarding the reliability and updating of the data. However, the fact that notaries authenticate the majority of instruments relating to the creation and existence of legal persons increases the reliability of the information. Information available essentially includes the legal ownership of the legal person, which may coincide with the beneficial ownership. Other means exist which aid in establishing beneficial ownership, in particular information obtained by financial institutions and DNFBPs, or any publicly available information on publicly and non-publicly traded Belgian companies. The

Effectiveness

effectiveness of ML/TF investigations involving legal persons or in which beneficial ownership information had been sought and used could not be established on the basis of the qualitative information provided by criminal prosecution authorities.

The sanctions imposed on persons who do not comply with obligations to provide transparent information on legal persons are not effective or dissuasive. Belgium has expanded its arsenal of sanctions in order to compensate for the ineffectiveness of administrative and criminal penalties, and the initial results are promising.

The development of legal arrangements in Belgium is limited. For this reason, the authorities have not at present identified or evaluated the vulnerabilities of such structures in relation to ML in Belgium. However, a risk analysis of fraud using foreign legal arrangements by natural persons subject to tax in Belgium has led to the tightening of reporting obligations to fiscal authorities on links to legal arrangements, including foreign ones. Professional trustees are as a general rule subject to AML/CFT obligations.

International co-operation with regard to the identification and exchange of information on legal persons and legal arrangements is generally positive in both directions (incoming and outgoing).

6. Financial Intelligence

Substantial

Within the Belgian legal system, competent authorities have at their disposal a wide range of measures for obtaining financial information and any other information pertaining to ML/TF investigations, both for obtaining evidence of offences and searching for and locating the related assets.

The CTIF collects information on ML and TF on a broad scale, and the processes used to gather the information are of high quality. The CTIF uses a large number of databases and maintains co-operation with all national and international authorities that can contribute or provide added value. The CTIF also carries out vulnerability analyses on the sectors subject to the obligations and shares the results with all relevant parties and authorities. Its reports are well-received and useful to the criminal prosecution authorities.

While criminal prosecution authorities use and gather information both for investigations and for prosecution, they do not do so in an optimal manner. Limited human resources do not allow criminal prosecution authorities to exploit all of the information received correctly or to build on it to reveal ML cases, in particular significant international cases.

7. ML Investigation and Prosecution

Moderate

The Belgian authorities possess a strong culture of fighting ML. They also have the necessary investigative techniques at their disposal. As a result, the number of prosecutions for ML is significant in Belgium. It is not uncommon for convictions to be obtained without a proven predicate offence due to the shared burden of proof in certain ML cases. However, The offences prosecuted are most often focussed on the predicate offences with a related ML charge against the same person. The number of cases of structured ML schemes involving third parties who facilitate the laundering of proceeds from offences committed by criminals is rare. Some offences, e.g. for the cross-border movement of cash, precious metals or diamonds, are under-prosecuted with respect to the level of risk indicated by Belgium.

Effectiveness

The scope of AML actions is limited by the absence at the national level of an overall strategy for combatting ML and lack of co-ordination between judges handling ML cases. A lack of resources, material means, training and co-ordination within the criminal prosecution agencies impairs their effectiveness. Too many cases are dismissed at the court's discretion, bringing down the rate of penal response. Furthermore, the length of certain ML procedures has the consequence that offences are not prosecuted within the statute of limitations, or the sanctions are reduced.

However, in preparing for and taking part in the assessment, the Belgian authorities identified shortcomings and demonstrated commitment to strengthening the prosecution of laundering as a priority, and produced examples of progress in this direction.

8. Confiscation

Moderate

The information provided by the Belgian authorities shows that seizure, confiscation and corresponding value confiscation are implemented in ML cases. However, while the authorities want to prioritise prosecutions giving rise to confiscation, they do not always fully succeed in this. The criminal prosecution authorities affirmed that there is an emphasis on confiscation, but the information provided did not show that goals consistent with this approach had been set. There is furthermore no evidence that financial investigations systematically include looking into assets that could be confiscated; it is available and easily identifiable proceeds that are regularly confiscated. The ineffectiveness in the criminal prosecution system (drawn-out procedures, statutes of limitation, etc.) also hampers confiscation.

The Belgian authorities do not have clear, relevant and centralised statistics on

- assets seized and confiscated in Belgium and abroad,
- asset sharing,
- the offences giving rise to these measures (ML and predicate offences),
- confiscation in cases of false disclosure or false declarations at the border, and
- the sums returned to victims.

This makes it difficult to assess the results of the investigations undertaken and performance in these areas.

9. TF Investigation and Prosecution

Substantial

The tactics and methods used by the Belgian authorities are not solely focused on the financial aspects of the global terrorist threat, but nothing in the actions they have undertaken, or the judicial rulings handed down, suggested to the assessors that these authorities are neglecting CFT. Based on the information the assessors received and interviews with the relevant specialists, it appears that the response of the Belgian authorities corresponds to the reality of the situations and threats, effectively detecting related offences and playing an active role in CFT. Persons have been convicted for TF within the scope of broader terrorism cases.

Effectiveness

10. TF Preventive measures & financial sanctions

Moderate

Belgium has a legal system allowing for the use of targeted financial sanctions in TF matters. However, the technical deficiencies found (notably the time it takes to implement new sanctions) raise doubts as to the system's effectiveness. In practice, the amount of assets that have been frozen is small, but this in itself is not an indication of ineffectiveness, especially because it has not been established that the assets concerned by the sanctions were on Belgian territory.

In terms of the risks of using NPOs for terrorist or TF purposes, there are shortcomings in the areas of administrative supervision regarding obligations on the transparency of NPOs, raising awareness, and targeted actions. However, the Belgian authorities have identified the NPOs that are at risk and set up ongoing monitoring of their activities and transactions.

11. PF Financial sanctions

Moderate

The Belgian legal system, coupled with that of the European Union, serves as the basis for implementation of the resolutions of the United Nations Security Council on targeted financial sanctions to counter the financing of proliferation. However, the time it takes to transpose such measures impairs the system's effectiveness. Even before they are transposed into European and therefore Belgian law, the information needs to be quickly communicated beyond the major financial institutions, and training and supervision measures are needed for all sectors subject to the obligations. The actions undertaken to thwart attempts to evade sanctions indicate that the various competent authorities all have high and appropriate levels of expertise and knowledge, although it is regrettable that more emphasis has not been placed on the financial component of proliferation.

Table 2: Compliance with FATF Recommendations

Compliance with FATF Recommendations			
Recommendation		Rating	Factor(s) underlying the rating
1.	Assessing risks & applying a risk-based approach	LC	<ul style="list-style-type: none"> • There is no formal mechanism for disclosing the non-confidential results of the risk assessment to the competent authorities and self-regulatory bodies as well as to the businesses and professions subject to the obligations. • Situations in which exemptions from AML/CFT obligations are allowed, and in which simplified measures can be applied, are not based on assessments showing low or lower risk. • Supervisors need to make more effort to ensure that obligated entities implement their AML/CFT obligations, taking risk into account.
2.	National cooperation and coordination	LC	<ul style="list-style-type: none"> • The principle of a national AML/CFT policy has been institutionalised but not yet put into effect.
3.	Money laundering offence	C	The Recommendation is fully met.
4.	Confiscation and provisional measures	C	The Recommendation is fully met.
5.	Terrorist financing offence	LC	<ul style="list-style-type: none"> • It does not appear to be an offence to supply funds to one or two persons without proof of a connection to a specific terrorist offence.
6.	Targeted financial sanctions related to terrorism & TF	PC	<ul style="list-style-type: none"> • Belgium is not yet able to apply the targeted financial sanctions of UNSCRs 1988 and 1989 without delay, which also compromises the application of sanctions without notice (de facto) to the entities concerned. • There is no formal mechanism at EU level or in Belgian legislation to request that other countries give effect to freezing actions undertaken according to UNSCR 1373.
7.	Targeted financial sanctions related to proliferation	PC	<ul style="list-style-type: none"> • Belgium is not able to apply the targeted financial sanctions of UNSCRs 1718 and 1737 without delay, which also compromises the application of sanctions without notice (de facto) to the entities concerned. • Sanctions for failure to comply with freezing obligations are not applied in a clear manner.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
8.	Non-profit organisations	PC	<ul style="list-style-type: none"> • There are shortcomings with regard to the initiatives to raise awareness and inform the NPO sector of TF risks. • Controls regarding transparency do not cover all of the components of R 8. • The proportionality of applicable sanctions has not been established.
9.	Financial institution secrecy laws	C	The Recommendation is fully met.
10.	Customer due diligence	LC	<ul style="list-style-type: none"> • Applicable provisions for determining beneficial ownership do not specify whether the financial institution must automatically consider the senior managing official as the beneficial owner when no natural person can be identified as such (and in cases where the administrator is separate from the senior managing official). • There is no explicit provision requiring financial institutions to systematically consider the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures apply.
11.	Record keeping	C	The Recommendation is fully met.

Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
12. Politically exposed persons	PC	<ul style="list-style-type: none"> The definition of PEPs does not include domestic PEPs or persons entrusted with a prominent function by an international organisation, as only persons living abroad who are, or have been, entrusted with prominent public functions can be considered PEPs. The list of persons to be considered direct family members and close associates of PEPs is too restrictive and contrary to the open, non-restrictive spirit of R 12. There is a time limit of one year, after which a PEP no longer exercising a prominent function should no longer be considered a PEP. In this case, the general principle applies, by which enhanced measures must be implemented if called for by the level of risk. There is no specific provision requiring the verification of whether the beneficiary of an life insurance contract or its beneficial owner are PEPs.
13. Correspondent banking	PC	<ul style="list-style-type: none"> Specific CCD measures for cross-border correspondent banking do not extend to relations with financial institutions of the European Economic Area (EEA) or an equivalent third country.
14. Money or value transfer services	LC	<ul style="list-style-type: none"> There is no clear policy on sanctions applying to persons who provide MVTS without being certified or registered, which would enable the proportionality of these sanctions to be determined.
15. New technologies	LC	<ul style="list-style-type: none"> Belgium has not developed a specific analysis of the ML/TF risks in the financial system due to the use of new technologies. However, the general AML/CFT framework does address these risks to some degree, through the application of enhanced due diligence rules applying to contracts entered into without face-to-face contact, and through the definition of 'specific risk criteria' which are the basis of the risk-based approach and for initial definition of the customer's risk profile.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
16.	Wire transfers	PC	<ul style="list-style-type: none"> The EC Reg. 1781/2006 does not stipulate the obligation of including information on the beneficiary of the transfer, and contains limited requirements for the obligations applying to intermediate financial institutions.
17.	Reliance on third parties	PC	<ul style="list-style-type: none"> It is not possible to verify whether the AML/CFT measures carried out by institutions are adequate due to the exemption for third party introducers from the EEA or third country equivalents. The inclusion of a country on the list of third country equivalents covers risk-related elements (compliance with the main FATF Recommendations, the level of risk relating to the amount of crime in the country), but this analysis is not focused on ML/TF risks.
18.	Internal controls and foreign branches and subsidiaries	PC	<ul style="list-style-type: none"> Only financial groups headed by a credit institution or investment firm are required by the law to develop a co-ordinated AML/CFT programme. Laws and regulatory measures do not specify the effective content of the obligations to be set out in this programme, nor do they stipulate that the branches and subsidiaries of groups are required to follow AML/CFT rules compatible with the level of risk in the home country.
19.	Higher-risk countries	LC	<ul style="list-style-type: none"> Belgium does not have instruments at its disposal that allow it to take counter-measures against higher risk countries, except within the scope of an FATF decision.
20.	Reporting of suspicious transaction	C	The Recommendation is fully met.
21.	Tipping-off and confidentiality	C	The Recommendation is fully met.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
22.	DNFBPs: Customer due diligence	LC	<ul style="list-style-type: none"> Trust and company service providers are not covered by Belgian AML/CFT measures. The limits identified under R 10, R 12, R 15 and R 17 affect DNFBPs. CDD requirements (R 10 rated LC) are central to R 22, but only moderate shortcomings were observed. Moreover, the weaknesses with regard to reliance on third parties (R 17 rated PC) have less impact in the context of DNFBP activities.
23.	DNFBPs: Other measures	LC	<ul style="list-style-type: none"> The limits identified under R 18 and R 19 affect DNFBPs. In particular, there is no independent audit function for testing the AML/CFT system for any DNFBPs. However, because of the small size of the DNFBPs concerned, this shortcoming has a limited impact.
24.	Transparency and beneficial ownership of legal persons	LC	<ul style="list-style-type: none"> Belgium has not assessed horizontally the ML/TF risks associated with the various categories of legal persons created on its soil up-to-date. Legal persons (or their representatives) do not risk facing sanctions simply for submitting false or erroneous information when reporting their beneficial ownership to the professions concerned, but the consequences of these acts can be punishable by sanctions. It is difficult to assess the proportionality of the sanctions due to the absence of information on the sanction policy. Mechanisms put into place by Belgium do not ensure that the information on beneficial ownership is correct and up-to-date. The mechanism applicable in Belgium to nominee shares is insufficient to ensure that they are not misused.
25.	Transparency and beneficial ownership of legal arrangements	LC	<ul style="list-style-type: none"> There is no clear policy on the sanctions applying to professional trustees who fail to meet their AML/CFT obligations that would allow the proportionality to be determined.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
26.	Regulation and supervision of financial institutions	PC	<ul style="list-style-type: none"> The BNB and the FSMA have set up processes and tools for defining the prudential risk profile of the institutions they regulate, of which ML/TF is one element. For the BNB, the share of ML/TF risk identified for each institution is not well-established. For the FSMA, with the exception of <i>bureaux de change</i>, the scope and frequency of ML/TF controls are not specifically formalised according to the type and level of risk identified for each institution. The BNB and the FSMA regularly review the risk profile of the institutions they regulate, but the extent to which ML/TF risk affects this revision is not specified. FPS Finance, which is tasked with supervising a major European payment institution for fund transmission services provided in Belgium via Bpost, does not specify the applied method of supervision. This is also the case for FPS Economy, although the sectors it supervises are lower risk sectors (consumer loan and direct financing lease providers).
27.	Powers of supervisors	LC	<ul style="list-style-type: none"> FPS Economy and FPS Finance can only impose the AML/CFT sanctions provided for by law, which are limited to disclosure measures and administrative sanctions.
28.	Regulation and supervision of DNFBPs	PC	<ul style="list-style-type: none"> There are no 'fit and proper' provisions that apply to diamond dealers and real estate agents. As a general rule, when supervision programmes exist, they have been established without assessing risk individually for the different professionals and without referring to the risk in the sector. There is no indication of how the risk profile of the entities concerned affects the scope and frequency of the controls.
29.	Financial intelligence units	C	The Recommendation is fully met.
30.	Responsibilities of law enforcement and investigative authorities	C	The Recommendation is fully met.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
31.	Powers of law enforcement and investigative authorities	C	The Recommendation is fully met.
32.	Cash couriers	C	The Recommendation is fully met.
33.	Statistics	PC	<ul style="list-style-type: none"> The statistical tools relating to STRs and investigations are good, but those for ML and TF prosecution and convictions are not up-to-date. The data on property seized and confiscated are fragmented and unreliable. Statistics on international judicial co-operation are almost non-existent, even though ML/TF risks in Belgium are often international in nature.
34.	Guidance and feedback	LC	<ul style="list-style-type: none"> The competent authorities, particularly the CTIF, disseminate AML/CFT-related information and establish guidelines for entities subject to the obligations. However, no recent specific measures have been taken by FPS Finance, FPS Economy or the authorities that regulate a number of DNFBPs. The supervisory authorities do not take part or take the initiative in providing sectoral feedback in relation to the implementation of reporting obligations, on the basis of observations made during their inspections. Such actions might help reporting entities detect and report suspicious transactions.
35.	Sanctions	LC	<ul style="list-style-type: none"> A fairly diverse range of sanctions can be applied, within the specific framework of AML/CFT supervision or in the course of prudential supervision. However, when and how these sanctions can vary in scale and nature depending on relevant criteria could not be determined, making it difficult to assess proportionality. When sanctions are imposed on legal persons, their directors can also be sanctioned. For some DNFBPs, this means a disciplinary penalty is imposed on the director.
36.	International instruments	C	The Recommendation is fully met.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
37.	Mutual legal assistance	LC	<ul style="list-style-type: none"> • Belgium lacks clear procedures for prioritising and executing requests for mutual legal assistance. • Moreover, the current system of managing cases does not allow for follow-up or monitoring the execution of rogatory commissions.
38.	Mutual legal assistance: freezing and confiscation	LC	<ul style="list-style-type: none"> • The expeditious nature of measures taken in response to identification and confiscation requests could not be established (see R 37).
39.	Extradition	LC	<ul style="list-style-type: none"> • Because there is no tool for managing requests, extradition requests cannot be ranked according to priority. Moreover, as the procedures for extraditions outside the EU are complex and unwieldy, extraditions without delay cannot be guaranteed. • When Belgium does not extradite its nationals based solely on their Belgian nationality, it is not guaranteed that these persons will be prosecuted.
40.	Other forms of international cooperation	LC	<ul style="list-style-type: none"> • Two of the supervisors (FPS Economy and FPS Finance) are not able to co-operate with foreign authorities with comparable responsibilities. • Belgium does not have an organised system for the exchange of information between non-counterparts.

Mutual Evaluation of Belgium

Preface

1. This report summarises the AML/CFT measures in place in the Kingdom of Belgium as at the date of the on-site visit. It analyses the level of compliance with the *FATF 40 Recommendations* and the level of effectiveness of Belgium's AML/CFT system and recommends how the system could be strengthened.
2. This evaluation was based on the *2012 FATF Recommendations*, and was prepared using the *2013 Methodology*. It was based on information provided by Belgium and information obtained by the evaluation team during its on-site visit to Brussels from 30 June to 15 July 2014.
3. The evaluation was conducted by an assessment team consisting of:
 - Mr Olivier Lenert, National Member for Luxembourg, Eurojust (legal expert)
 - Mr Patrick Lamon, Chief Federal Prosecutor, Public Ministry of the Swiss Confederation (operational expert)
 - Mrs Khadija Medjaoui, Legal professional, French banking supervisor (*Autorité de Contrôle Prudentiel et de Résolution*), France (financial expert)
 - Mr Diego Bartolozzi, Head administrator, Financial Information Unit, Bank of Italy (financial expert)
 - Mrs Livia Stoica-Becht, Unit manager, MONEYVAL Secretariat (expert / observer)
 - Mr Emmanuel Mathias, Senior Financial Sector Expert, International Monetary Fund (expert / observer)
 - Mr Vincent Schmoll, Mrs Anne-Françoise Lefèvre and Mrs Gwenaëlle Le Coustumer of the FATF Secretariat.¹
4. The report was reviewed by Mrs Marie-Élisabeth Lebrun, Finance Canada (Canada); Mr António Gageiro, Securities Market Commission (Portugal) and Mr Jean-Pierre Brun (World Bank).
5. Belgium previously underwent an FATF mutual evaluation in 2005, conducted according to the *2004 FATF Methodology*. The 2005 evaluation was published and is available on the FATF website (www.fatf-gafi.org). For the sake of brevity, on those topics where there has not been any material change in the situation of Belgium or in the requirements of the *FATF Recommendations*, this evaluation does not repeat the analysis conducted in the previous evaluation, but includes a cross-reference to the detailed analysis in the previous report.
6. Belgium's 2005 mutual evaluation concluded that the country was compliant (C) with 21 Recommendations, largely compliant (LC) with 20 Recommendations, partly compliant (PC) with 6 Recommendations, and non-compliant (NC) with Special Recommendation (SR) IX, bearing in mind that Recommendation 34 was not applicable. Belgium was rated C or LC with 14 of the 16 Core and Key Recommendations (Recommendations 23 and SR III, which were among the Key Recommendations, were rated PC). For this reason, Belgium was not placed under the follow-up process but did submit updates every 2 years starting in June 2007.

1 Mrs Catherine Marty also took part in the analysis of technical compliance.

1. ML/TF RISKS AND CONTEXT

1.1. **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. In 2013, the gross domestic product (GDP) was EUR 395.2 billion.¹ The capital of Belgium is Brussels.

1.2. **Belgium is a constitutional monarchy and a Federal State.** The King is the Head of State but does not hold executive power. The executive federal power is held by the Prime Minister and his 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.

1.3. **The Federal Government's authority covers areas (such as foreign affairs, national defence and justice), including AML/CFT.** The Belgian population is broken down into three linguistic groups, which are institutionally organised into three *communities*: the Flemish-speaking Community, the French-speaking Community and the German-speaking Community. Belgium is also made up of three economic *regions*: the Brussels-Capital Region, the Flemish Region and the Walloon Region. Each region and community has the executive and legislative power to pass measures (decrees, orders) that have the force of law 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 (e.g. rolled sheet steel), they play a role in countering the financing of proliferation of WMD (FP).

1.4. **Belgium is one of the six founding Member States of the European Union (EU).** The European Commission and the majority of community institutions are headquartered in Brussels. The AML/CFT regime in Belgium is based on a legal framework defined at both the national and European level.

1.1 ML/TF Risks

1.5. **This part of the MER summarises the assessment team's understanding of the ML/TF risks in Belgium.** It is based on the documents provided by Belgium, publicly accessible documentation and interviews with the competent authorities and the private sector during the on-site visit.

1.6. **With regard to ML, Belgium is considered a transit country for illegal funds.** The main ML activities are layering (notably internet fraud cases), then integration and placement. Laundered funds in terms of the number of cases transmitted by the CTIF to the prosecution authorities between 2008 and 2012 were mainly related to fraud (in particular through the internet), offences related to bankruptcy fraud and misappropriation of corporate assets. In terms of the amounts laundered, the main predicate offences include tax fraud, organised crime (often linked to illicit trafficking of narcotics or property), fraud and illicit trafficking of property and merchandise. There is also a regular increase in STRs relating to economic and financial crime (e.g. offences relating to bankruptcy fraud, misappropriation of corporate assets, illegal labour trading and tax fraud).

1.7. **While the banking sector continues to be the focus of the largest detected ML transactions, criminals are increasingly turning to new sectors, such as the precious metals market.** Use of cash is a major vector for ML in Belgium, fuelling the underground economy (estimated at 16.8% of the GDP²). Activities that typically handle large sums of cash are particularly vulnerable (e.g. used car sales, antique and art dealers, night shops). The fund transfer sector also faces risks in this context.

1 OECD (nd).

2 European Commission (2012).

1

1.8. High risks were also identified in certain transactions involving gold and precious metals (copper, platinum, zinc), partly due to the associated use of cash. Due to its central position in Europe, Antwerp's position as a major port, and its status as a transit country, Belgium is also exposed to illegal cross-border movements of funds. Given Antwerp's position as the centre of the world diamond trade,³ the value and transportability of diamonds, and the volumes traded, the diamond sector also represents a significant risk.

1.9. **Misuse of legal persons, particularly for tax fraud and benefit fraud, is another area exposed to risk.** The risk is aggravated by the fact that legal and tax consultation services for pre-establishment and company matters are provided by persons who are not subject to any AML/CFT obligations. The possible involvement of certain legal and financial professionals, a risk pointed out in the national ML risk assessment, is also of concern.

1.10. **There is also a risk of TF with the presence of certain groups in Belgium.** The presence of these groups from countries where there are ongoing wars, national independence movements and terrorist phenomena creates a location for recruitment or fund raising that is tapped to finance terrorist organisations, mainly for operations abroad. The risks in terms of TF seem to involve not only structural terrorist financing, but also simple operations on an individual scale, such as the activities of *ihadists* who have gone to countries in the Near and Middle East. Recent events in these regions and the continuing phenomenon of radicalisation in certain segments of the population create undeniable risk. The fund transfer sector is particularly vulnerable to these threats.

1.2 Materiality

1.11. **Belgium is an open economy and a member of the euro zone.** Belgium has the sixth largest economy in the euro zone (which included 18 of the EU Member States in July 2014) and represented 4% of the zone's GDP in 2013. Its economy is service-dominated, in similar proportions to other EU Member States.⁴ Its average in imported and exported goods and services (in percentage of the GDP) stood at almost 80% in 2010, almost twice the EU average, which is a testament to both the open nature of the Belgian economy and its exposure to incoming and outgoing financial and non-financial flows.⁵

1.12. **The rate of taxation in Belgium is very high:** In 2011, the average tax wedge was 50% for an unmarried person with no children (the highest rate among all OECD member countries⁶). Moreover, while the tax burden on company earnings is quite moderate (6.4%), social security contributions represent an average of 50.3% of gross wages.⁷ These rates tend to contribute to benefit and tax fraud, which can lead to ML.

3 In 2013, diamond imports represented EUR 20 billion, and diamond exports approximately EUR 22 billion – Figures from the FPS Economy.

4 Gross added value of different sectors, in percentage of GDP (2010): financial activities and business services (30%); industry including energy (16.4%); commerce, transport and communications (21.6%); construction (5.3%); and other activities and services (25.1%), Eurostat.

5 Assessment of ML threats, risks and vulnerabilities, December 2013, p. 11.

6 *OECD Economic Studies: Belgium*, May 2013; p. 23. The notion of tax wedges is used to measure the difference between what employers pay in the form of wages and social security contributions, and what employees are left with after the deduction of taxes and social security contributions, also taking into account cash transfers attributed through public social aid programmes.

7 Pricewaterhouse Coopers (2014), p. 157.

1.13. **The financial sector in Belgium is relatively integrated, and for the most part credit institutions are part of major multinational financial groups.** During the financial crisis in 2008, the Belgian state bailed out three large credit institutions, and the process of internalisation and consolidation of the Belgian banking system accelerated. Today, three of the country's five largest banks (balance sheet total) are Belgian subsidiaries of foreign groups, two of which are within the EU. In 2012, the total bank assets amounted to EUR 1 048.7 billion, i.e., 288.7% of the GDP,⁸ which places Belgium at the lower end of the European spectrum in terms of its economy's exposure to systemic risk in banks. The IMF FSAP assessment carried out in 2013 observed the progress made by Belgium in stabilising its financial sector, as reflected by the ability of the large institutions to withstand scenarios of economic or financial shocks to which the Fund subjected them. The assessment also highlighted the high degree of compliance by Belgium with international best practices dealing with banking and insurance supervision.

1.14. **The diamond sector is of particular importance, along with Antwerp's position as the largest diamond trading centre in the world, particularly for uncut diamonds.** It is estimated that around 84% of the global production of uncut diamonds are traded in Antwerp, as well as 50% of polished diamonds.⁹ In 2012, the city's diamond trade represented a total of USD 51.9 billion, i.e., the equivalent of USD 200 million in diamonds passing through Antwerp every day. Diamonds represent approximately 5% of Belgian exports and approximately 15% of all Belgian exports outside the EU, but according to FPS Economy, the sector represents only 0.5% of the GDP if the value added in Belgium is taken into account. Diamond dealers account for 1 700 businesses, of which 19% are individual enterprises and approximately 65% are small and medium-sized businesses.

1.3 Structural Elements

1.15. **The structural elements needed to ensure an effective system of preventing and combatting ML/TF are present in Belgium.** There is a relative political stability, despite the difficulties encountered in forming a federal coalition government which has delayed certain AML/CFT decisions (see Section 2), and a high level of political commitment to addressing AML/CFT issues. Belgium is equipped with stable institutions which are held accountable. Belgium is a country that adheres to the rule of law with a competent, independent judicial system, although the effectiveness of this system is limited by a lack of resources.¹⁰ With its institutional structure, Belgium is equipped with the necessary framework for implementing its AML/CFT regime. Responsibility for developing and implementing the AML/CFT policy in Belgium is shared between the competent authorities whose statuses and roles are well-defined (see Section 2, point 2.1.(b)).

1.4 Other Contextual Factors

1.16. **The AML/CFT regime in Belgium is based on a legal framework defined both at the national and European level.** European AML/CFT regulations apply directly in Belgium and add to the legislative and regulatory measures taken by the authorities to transpose the 3rd European Directive on AML/CFT (2005/60/EC) into national law. The draft of the 4th European Directive – aimed at adopting the changes made to the FATF rules in 2012 – was in the process of being passed at the time of the evaluation, and therefore was not taken into account in this analysis. To avoid making repeated changes to their legal system, the Belgian authorities have decided to revise the national AML/CFT regime only once, and therefore to wait until the 4th Directive has been adopted to adapt the national regime to both the revised FATF Recommendations and this new Directive.

8 Febelfin (2012 and 2014).

9 Antwerp World Diamond Centre, (2013).

10 On this matter, see the risk assessment which refers to the OECD report on corruption: Phase 3 Report on implementing the OECD Anti-Bribery Convention in Belgium (OECD, 2013), mentioned in the Assessment of ML threats, risks and vulnerabilities, December 2013.

1.5 Scoping of Issues of Increased Focus

1.17. **During their preparatory work, the assessors identified several topics requiring particular attention.** They did this by analysing the ML and TF risk assessments done by the Belgian authorities and studied the available information on the legal and institutional environment, among other things, and the context surrounding ML/TF risks in Belgium, including potential points of vulnerability. The following list of elements – the scoping note¹¹ – was submitted to the Belgian authorities prior to the on-site visit, and these elements were discussed at length with the Belgian experts met during the visit.

Institutional and structural aspects

- *Control systems aimed at detecting and dissuading violation of AML/CFT obligations*, particularly for the sectors considered most vulnerable (diamond dealers, casinos, legal, accounting/tax and real estate professions); resources allocated to supervision of all entities subject to the obligations; and the applicable sanctions.
- *Criminal prosecution and suppression of ML*, obstacles such as insufficient material means and expertise allocated to prosecution authorities appear to hinder or compromise their efforts to counter and prosecute ML; as well application of the sanctions.
- *Seizure and confiscation*, hindered by the lack of resources allocated to the justice system (prosecutors' offices and courts) to combat organised and white collar crime.
- *Vulnerability of legal persons with regard to ML*, particularly the use of company structures for criminal purposes; the criminal law framework, and criminal prosecutions and convictions of legal persons; and access to information on beneficial ownership and supervision of professionals involved in the establishment of legal persons.
- *Prevention and suppression of TF*, particularly lack of resources for enforcement authorities and weaknesses in the legal framework for the freezing of funds related to terrorist organisations and the implementation of targeted financial sanctions.

Aspects relating to specific areas and business sectors

- *Prosecution and criminalisation of serious tax fraud*, a priority for the Belgian authorities and the subject of recent legislative measures.
- *Circulation of cash*, still widespread in Belgium, notably in relation to the gold trade, which is therefore particularly vulnerable to ML/TF risk, but which also feeds formal and informal fund transfer systems; and finally the adequacy of means of detecting violations of restrictions on payments in cash.
- *Vulnerabilities in the diamond sector*, given Antwerp's position as the centre of the world diamond trade and the detection of cases of illegal diamond trafficking and large-scale tax fraud involving diamond dealers.

11 See Methodology, para. 44 on the scoping note, and Procedures for the 4th cycle of evaluations, para. 26 (FATF, 2013).

Bibliography

- Antwerp World Diamond Centre (2013), *Risk analysis of the Antwerp diamond sector*, Antwerp World Diamond Centre, November 2013.
- European Commission (2012), *Shadow Economy and Undeclared Work*, European Commission, http://ec.europa.eu/europe2020/pdf/themes/07_shadow_economy.pdf
- FATF (2013), *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%202022%20Feb%202013.pdf
- Febelfin (2012), "2012 data", *Chiffres individuels par banque*, Febelfin, Brussels, www.febelfin.be/fr/chiffres/chiffres-individuels-par-banque
- Febelfin (2014), *Key data from 2012-2013*, Febelfin, Brussels, www.febelfin.be/sites/default/files/files/ff_fr_2014_gmr.pdf
- OECD (nd), *Gross domestic product (GDP)*, OECD.Statextracts, Paris, http://stats.oecd.org/Index.aspx?DataSetCode=SNA_TABLE1&Lang=en
- OECD (2013), *Phase 3 Report on Implementing the OECD Anti-Bribery Convention in Belgium*, OECD Paris, www.oecd.org/daf/anti-bribery/BelgiumPhase3ReportEN.pdf
- Pricewaterhouse Coopers (2014), *Paying taxes 2014*, Pricewaterhouse Coopers, www.pwc.com/gx/en/paying-taxes/assets/pwc-paying-taxes-2014.pdf

1



2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings

Belgium has established a framework for assessing the threats and vulnerabilities associated with ML/TF and for national co-operation and co-ordination.

Belgium appears to understand its TF risks correctly and is taking co-ordinated action to attenuate these risks at the national level. There is also good co-ordination in combatting the financing of proliferation.

Although ML risks appear to be identified and understood overall, their analysis has not benefited from a proactive approach, notably in focussing on vulnerabilities.

Elements of a risk-based approach have long fed into AML polices and activities. The CTIF and, to a large degree, the law enforcement authorities (particularly the police) have traditionally considered the identified risks when defining their objectives and activities.

At the time of the on-site visit however, co-ordination at the national level was hampered by :

- the failure of supervisory authorities and self-regulatory bodies to incorporate the main risks of ML/TF into their oversight policies;
- the failure to address a certain number of ML risks appropriately; and
- the incomplete dissemination of the non-confidential results of the risk assessments to financial institutions and DNFBPs, thus slowing down their being taken into account in internal procedures.

2.1 Background and Context

(a) Overview of the AML/CFT Strategy

2.1. **By creating a co-ordinating mechanism in 2013, Belgium strengthened the system it uses to develop and co-ordinate its AML/CFT policy.** Prior to that, the CTIF had been responsible for developing AML/CFT policy and measures and for co-ordination in this area. Since 2008, the College for combatting tax social benefits fraud also co-ordinated elements of the AML strategy related to its areas of responsibility. The CCLBC, newly established (see below) has communicated the results of the ML risk assessment to the Minister of Justice, who has asked for both legislative and operational concrete proposals , , to be developed as a basis for initiatives by the new federal government (see 2.3 (b)). At present, Belgium does not have an overall long-term AML/CFT policy.

(b) The Institutional Framework

2.2. As regards ministries and operational agencies, the institutional framework in Belgium described in the 2005 MER (para. 54 - 94) remains unchanged. Their roles and responsibilities essentially remain the same:

■ Ministerial level:

- the Prime Minister (general policy),
- the Ministers of Justice and Finance (authorities jointly in charge of supervising the Belgian financial intelligence unit [FIU] known as the *Cellule de Traitement des Informations Financières* [Financial Intelligence Processing Unit] – CTIF), and
- especially some of the Belgian ministries, (Federal Public Services [FPS]):
 - FPS Finance (particularly tax fraud and freezing of TF assets),
 - FPS Justice (criminal policy and criminal investigations),
 - FPS Interior (particularly the TF threat),
 - FPS Economy (particularly registering Belgian businesses and restricting cash payments), and
 - FPS Foreign Affairs (countries subject to embargoes);

■ Operational agencies:

- the CTIF (Belgian FIU),
- the Federal Police (investigations and support for inquiries),
- the Federal Prosecutor's Office (co-ordinating public action),
- the Central Office for Seizure and Confiscation (*Organe Central pour la Saisie et la Confiscation - OCSC*),
- the State Security Service (*Sûreté de l'État -- SE*),
- the General Service for Intelligence and Security (*Service Général du Renseignement et de la Sécurité -- SGRS*), and
- the Customs & Excise (*Administration Générale des Douanes et Accises -- AGDA*) (embargoes).

2.3. **Substantial changes nevertheless took place in 2010 regarding the division of responsibilities for ML/TF supervision** (see Section 6, point 6.1. and Section 5, table below point 5.1.(b)):

- As regards financial companies, as part of a general reorganisation of the framework for prudential supervision in 2010, the National Bank of Belgium (BNB) and the Financial Services and Markets Authority (FSMA) took back the supervisory powers for AML/CFT previously devolved to the Banking, Finance and Insurance Commission (*Commission Bancaire, Financière et des Assurances - CBFA*);
- The CTIF's responsibility for the AML/CFT supervision of designated non-financial businesses and professions (DNFBPs) was transferred to the supervisory, oversight or disciplinary authorities for the relevant businesses and professions.

(c) *Co-ordination and Co-operation Arrangements*

2.4. **A new mechanism for co-ordination between the authorities involved in AML/CFT came into force in 2013.** It formalises existing co-operation and co-ordination mechanisms and is intended to regularly update the assessments of the ML and TF risks and determine the national AML/CFT policies. This approach aims to meet the FATF's new requirements.

2.5. **This mechanism is based on concerted action within and between two Ministerial Committees, one specialising in ML, the other addressing TF** and the financing of proliferation of weapons of mass destruction (PF):

- i. the *Ministerial Committee for co-ordinating measures against laundering money from illegal sources* (created by Royal Decree [RD] of 23 July 2013) which establishes the general policy on AML and sets the priorities of the services involved in countering it; and
- ii. the *Ministerial Committee for intelligence and security* (RD of 23 July 2013, amending the RD of 21 June 1996 on the creation of a Ministerial Committee for intelligence and security), responsible for defining the government's general TF and PF policy.

2.6. **The Ministerial Committee responsible for countering ML is chaired by the Minister of Justice and includes members of the government** who have responsibilities for finance, the interior, the economy, small and medium enterprises (SMEs) and for co-ordinating countermeasures to fraud. A College (*Collège de coordination de la lutte contre le blanchiment de capitaux d'origine illicite - CCLBC*) associated with the Minister of Justice has been created to monitor the general implementation of the AML policy, as defined by the Ministerial Committee. The CCLBC is chaired jointly by the President of the CTIF and by the Prosecutor General responsible for financial, tax and economic crime. It consists of an *Assembly of Partners*, a Judicial Platform and a Joint Unit. The role of the *Assembly of Partners* is to identify and analyse the ML risks confronting Belgium: its role is preventive. It is chaired by the President of the CTIF, and its members include representatives from the FPSs for finance, the economy and justice, the BNB, the FSMA, the College of Prosecutor Generals, the CTIF, the Federal Police and the Standing Commission for the Local Police. The Assembly of Partners can on its own initiative decide to consult other bodies or authorities if it considers that this might facilitate its work. For instance, it decided in December 2013 that henceforth the National Security Service should be invited to attend its meetings. The purpose of the Judicial Platform is to co-ordinate the related enforcement policy. The role of the Joint Unit is to ensure that all measures implemented (both preventive and punitive) are consistent, and to propose to the Ministerial Committee what action to take.

2.7. **The Ministerial Committee for Intelligence and Security is chaired by the Prime Minister and includes other members of the government:** The Minister of Foreign Affairs, the Minister of Justice, the Deputy Prime Minister and Minister of Defence, the Minister of Interior and the Ministry for Economy. The Committee is responsible for defining the government's general policy for intelligence and security, and since 2013, its policy on countering TF and PF. Committee decisions are implemented by a College (*Collège du renseignement et de la sécurité - CRS*), which is an administrative body acting as an intermediary between the Ministerial Committee and the services applying the policy for intelligence and CFT (and PF) operationally. Among the services responsible for applying this policy in practice are the Federal Prosecutor's Office, the

State Security Service, the General Service for Intelligence and Security Service, AGDA, the Central Unit for Threat Assessment (*Organe central pour l'analyse de la menace -- OCAM*), the CTIF and the TF Unit of the Federal Police's Central Service for Terrorism and Sects. The College is also responsible for analysing the risks of TF.

2.8. **These co-operation mechanisms are supplemented by measures that organise co-ordination at an operational level.** This includes in particular agreements between the CTIF, the other State agencies and the judicial authorities describing how information is exchanged (see R 29 and Section 3). The CTIF hosts liaison officers from other State services (such as the Police and AGDA). The Federal Police have also developed co-ordination methods and procedures, particularly with the Customs Administration. In 2003, the College of Prosecutors-General created 'Ecofin', a network of expertise in countering economic, financial and tax crime (including ML). It helps draft and implement criminal policy (see MER 2005, para 70). The BNB and the FSMA have also arranged to exchange information via a protocol covering countering ML/TF (see Section 6).

(d) Country's Assessment of Risk

2.9. **Belgium has conducted two national risk assessments, in December 2013 for ML and in February 2014 for TF.** These two documents summarise the knowledge of threats and vulnerabilities related to ML/TF developed over the last few years by different authorities.

2.10. **The assessment of the threat and risks relating to ML was carried out by the Assembly of Partners of the CCLBC.** It highlights the threats of ML and the predicate offences, the factors that aggravate the threats and risks, and makes recommendations to improve the system. The information is presented as it was provided by each authority, so that in this initial evaluation, the horizontal analysis of trends (i.e. of the potential impact that phenomena observed in one activity sector could have, directly or indirectly, on another) remains partial. Nevertheless, it provides a good basis for identifying the risks that Belgium faces.

2.11. **The assessment of TF risks was carried out by the CRS.** This second section of the national risk assessment refers to the ML risk assessment and extracts conclusions that apply to both phenomena (ML and TF). It follows the ML risk assessment in that the information is presented as it was provided by each authority. The contributions are followed by typologies studies illustrating the trends identified.

2.2 Technical Compliance (R 1, R 2, R 33)

Recommendation 1 - Assessing risks and applying a risk-based approach

2.12. **Belgium is largely compliant with R 1** – Measures are in place for assessing the risks in the country, and the necessary mechanisms for taking into account the evolution of these risks have been defined. Entities having obligations under the AML/CFT law are required to identify their ML/TF risks with a view to implementing adapted measures, core requirements of R 1. Nevertheless, certain elements are lacking, and in particular there are no mechanisms for ensuring the dissemination of the non-confidential results of the TF risk assessments to supervisors or to the businesses and professions subject to AML legislation. In addition, situations in which exemptions to the AML/CFT obligations are allowed and simplified measures may be applied, are not based on an assessment of low or lower risk. Finally, effort is needed by supervisors to ensure that obligated entities implement their AML/CFT obligations taking risk into account.

Recommendation 2 - National co-operation and co-ordination

2.13. **Belgium is largely compliant with R 2** – There is no national (overall) AML/CFT policy that takes into account risks that have been recently identified; however, basic elements of national co-operation and co-ordination (criteria 2.1 and 2.3) are essentially in place with a view to further development.

Recommendation 33 - Statistics

2.14. **Belgium is partially compliant with R 33** – The authorities have full statistics as regards reporting suspect operations and ML investigations, and partial statistics on TF investigations and on prosecutions and convictions related specifically to ML and TF. Statistics relating to frozen, seized or confiscated assets or to judicial co-operation are incomplete, and often the data collected by one authority is not comparable with that collected by another. There is a new IT system for judicial co-operation, but it covers only requests made outside the EU since 2013.

2

2.3 Effectiveness: Immediate Outcome 1 (Risk, Policy and Co-ordination)*(a) Country's understanding of its ML/TF risks*

2.15. **Since the 1990s, the Belgian AML framework has evolved in line with changes to the identified risks.** Thus, when the AML issue was first raised in 1993, the Belgian authorities identified the risk of tax fraud and its interaction with ML, and they progressively reinforced the legislative framework and co-operation between the CTIF and FPS Finance. Similarly, in 1996, the federal government approved an action plan to counter both organised crime and economic, financial and fiscal crime, that identified the risks posed by non-financial businesses and professions. These two aspects were not introduced into the FATF standard until 2003 and 2012 respectively. In addition, the College for combatting tax and welfare fraud was established in 2008.

2.16. **The national assessment of ML risks in 2013 is a further step** towards understanding the risks in their entirety. Before the CCLBC was created in July 2013, the CTIF was alone responsible for co-ordination. Identifying and analysing the ML risks that Belgium faces is now the responsibility of an Assembly of Partners (see above, point 2.1(c)). The phenomena and activities that make up the threats and, to a certain degree, the vulnerabilities of the country are identified. However, this has been done in a fragmented manner, since the report does not provide a synthesis of the observations made individually by each authority that contributed to it. The conclusions of the report do identify the types of criminal activity that are high-risk in relation to ML (financial crime, tax fraud) and the activities exposed to ML (cross-border transportation of cash, trade in precious metals, company structures). According to the findings of the evaluators (see point 1.1), these elements correspond to the areas that are particularly at risk for ML/TF.

2.17. **At this stage, the analysis of ML risks covers essentially the suspect operations detected.** The threat analysis is largely based on information collected by the CTIF (particularly on STRs), from the police and the judicial authority (especially those related to investigations and convictions), and from FPS Economy. This creates a bias towards certain phenomena that either have already been the subject of STRs received by the CTIF or have been addressed through criminal prosecution. This does not encourage the detection of new trends or the implementation of measures that might anticipate or slow down their emergence. For this reason and in the absence of confidential elements in the national ML risk assessment, the contribution of the intelligence services to the threat assessment is unclear, since the State Security service was only invited to meetings of the Assembly of Partners in December 2013 when the risk assessment had been finalised.

2.18. **Therefore, given that some authorities contributed little or not at all to the risk assessment, a comprehensive understanding of risks is not yet possible.** The threat analysis did not receive input from other potentially useful sources especially for the understanding of vulnerabilities, for example some AML supervisors not represented in the Assembly of Partners (such as those supervising the accounting/tax and legal professions and gambling). The contribution of financial supervisors (although members of the Assembly of Partners) has also been limited, which, given the use made of the financial sector for ML purposes, is detrimental to understanding. Added to this, the private sector was not asked to contribute to the work, as sectoral risk assessments have not yet been carried out (except for the diamond sector; see below). Nevertheless, it appears that some businesses and professions subject to AML legislation, particularly in the financial sector, already have a clear understanding of their ML/TF risks (see Section 5) and could usefully contribute. The authorities indicated however that the contribution of the CTIF, in particular, to the risk assessment benefited from the continuing contacts with the financial and non-financial professions. Lastly,

as regards quantitative input to the risk analysis, general statistical data held by the BNB and Statbel, such as changes in payment methods, the circulation of fiat money and the source and destination of international payments (e.g. from the Target2¹ database) were not used to attain a better understanding of vulnerabilities. The same applies to statistics available at European level from institutions such as Eurostat and the Central European Bank.

2.19. **Belgium has resources to analyse terrorist risk that have gradually incorporated aspects of TF.** The Ministerial Committee for Intelligence and Security has existed since 1996 and deals, inter alia, with terrorism. Its decisions are implemented by the CRS (see above, point 2.1(c)). Members of the CRS have gradually incorporated TF issues into their work. The Police, for example, have included TF as a priority since the 2008-2011 National Security Plan. For 2012-2015, the view of risk includes TF aspects prepared by OCAM. The agency is also responsible for the plan on radicalisation ('Plan R') which since 2005 has aimed to detect and monitor radical individuals, groups and media, and includes aspects of TF.

2.20. **However, the national assessment of TF risks does not appear to have benefited from the same attention as that conducted for ML risks.** The assessment draws only one specific conclusion: the need to implement existing national measures for asset freezing. Otherwise, it quotes the conclusions from the ML risk assessment considering that the other risks are under the purview of the Federal Prosecutor's Office and OCAM. Furthermore, not all the authorities with potentially useful information about TF have contributed to the assessment, in particular the AML/CFT supervisors. It is also regrettable that the CTIF is not a member of the CRS, even though until July 2013, it alone was in charge of co-ordinating CFT measures. Through the absence of the CTIF, the CRS is deprived of the direct participation of a long-standing player in CFT.² The CTIF did contribute to the assessment, but its contribution was not fully utilised in CRS's work.

2.21. **Despite shortcomings in the process for assessing TF risks, the main competent authorities appear to demonstrate an adequate understanding of the risk,** based on the actions and assessments they carry out at sectoral level. It also appears that sensitive information and some available analyses have not all been included for security and confidentiality reasons. The finding must nevertheless be qualified for supervisors, particularly in the non-financial sectors, who have not yet gone through a process to identify TF-related vulnerabilities.

(b) Managing the ML/TF risks identified

2.22. **Belgium was very early to include risk as a factor influencing AML policies and activities.** In 1995, serious tax fraud was introduced into the AML Law as a predicate offence for ML. In 1998, because of the risks identified in their activities, bailiffs, lawyers, company auditors, external chartered accountants, estate agents, cash transporters and casino operators became subject to AML legislation. Similarly, the enhanced risk in cash payments has led to their prohibition, for amounts over EUR 15 000 in 2004 under the AML/CFT Law, and over EUR 3 000 in 2014 (the same obligations have applied to service providers since 2012).³ Cash transactions are now prohibited for real-estate transactions. Lastly, because of the risks in diamond trading, the authorities have decided that traders must comply with the measures in the RD of 2013. These are more severe than those specified in the international standard because they apply to all transactions, not just cash, above a defined threshold (R 22c). The Belgian authorities know the risks of the diamond sector, and this knowledge enabled them to provide a critical contribution to the joint FATF / Egmont Group ML/TF typologies study on diamonds⁴.

1 Real-time euro-based gross settlement transfer system, developed and managed by the Eurozone countries.

2 The Belgian authorities have since indicated that the National Security Council, whose creation was announced in the Government Statement of October 2014 and which will be responsible for all security and intelligence issues, will include the CTIF among its members.

3 At the end of 2014, the government indicated that it intended to raise the threshold to EUR 7 500.

4 FATF and Egmont Group (2014)

2.23. **The risk-based approach has had positive results.** The VAT carousel fraud area is the best example in this regard. In 2001, the cost of VAT fraud was estimated at EUR 1.1 billion, and this prompted the formation in 2002 of a support unit (made up of police officers and tax specialists) in the taxation service's Special Investigations Unit. It compared tax data from national and international sources and reviewed the phenomenon in detail, in order to identify the different modus operandi used by criminals (including the ML consequent on the fraud). The approach has enabled the situation to be relatively well controlled, with losses reduced to EUR 18.5 million in 2012. The system has been recognised within the EU as the forerunner to an integrated approach to VAT carousel fraud.

2.24. **Not all of the risks identified in the past years have been addressed adequately.** It can thus be observed that the criteria for reporting suspicions of gaming operators have not been reviewed since 1999, despite the progress made internationally in understanding the risks in this sector, and the technological advances in on-line casinos. Furthermore, although the CTIF identified significant ML risks in company domiciliation and monetary gold in 2011 and 2012 respectively, these sectors still fall outside the AML/CFT framework. Finally, the revelation by the CTIF of the problems linked to shortcomings in the supervision of lawyers has not resulted in any action. One of the reasons for the difficulty in addressing these significant risks seems to be a lack of priority given to AML/CFT, as well as the absence of an overall, continuing and well-defined strategy for the authorities to prevent and combat ML and TF.

2.25. **The findings of the recent assessment of ML risk were beginning to feel their effect at the time of the on-site visit.** In January 2014, the principal conclusions were communicated to the Minister of Justice, who chairs the Ministerial Committee. The conclusions were supported by a short description of the main structural problems identified by the CCLBC: judicial resources and the effectiveness of controls and administrative sanctions. The use of cash and the cross-border transportation of cash were highlighted as areas that were not adequately addressed. Proposals and solutions to remedy the problems were also outlined. Following this communication, the Minister asked for concrete measures, both legislative and operational, to be developed before convening the Ministerial Committee. It should be noted that at the time of the on-site visit, the government had resigned (in May 2014) and could only deal with day-to-day business. Nevertheless, based on the conclusions in the risk assessment on the effectiveness of the legal system, the *Prosecutor General* for Brussels had already decided to create a group of 15 judges within his jurisdiction who are specialists in financial crime, including ML. The group should be operational from December 2014. For their part, AGDA has strengthened checks on cross-border transportation of cash. Despite the high risk associated with certain non-financial sectors, in particular lawyers, no measure was envisaged for reinforcing the AML/CFT controls of these activities.

2.26. **The TF risk assessment appears unlikely to influence the authorities' policies and activities,** since it lacks conclusions and recommendations other than those on implementing the rules for freezing of terrorist assets – the CRS is focussed on developing a Belgian list. Nevertheless, those members of the CRS that the assessment team met with, indicated that the current priority for CFT is to track people who move between Belgium and sensitive regions, such as Syria. The CRS plans to prepare concrete proposals based on the TF risk assessment. This being said, the relevant players in counter terrorism and CFT have developed CFT activities and policies that address the risks identified outside the framework of the TF risk assessment.

(c) Using the risk assessments to support exceptions to CDD rules

2.27. **The recent risk assessments have as yet had no impact on the legal framework for AML/CFT that applies to financial institutions and DNFBPs.** They have not led to waivers or to the application of reinforced or simplified measures. There is also no risk analysis showing that all the cases in Art. 11 of the AML/CFT Law present a low or lower risk (see criteria 1.7, 1.8 and 10.18 of the TC Annex).

(d) Alignment of the activities of the competent authorities and self-regulatory bodies with the national AML/CFT policies and the identified risks

2.28. **The CTIF has traditionally considered identified risks when defining its objectives and activities.** Apart from the points discussed above, the CTIF has developed a risk-based approach based on the national ML risk assessment for the operations involved in processing ML cases opened after suspicious

transaction reports. For instance, information shared by AGDA relating to risk assessment may be used to refine the CTIF's analysis criteria.

2

2.29. **The criminal prosecution authorities have recognised ML/TF risks in their objectives and activities to differing degrees.** Although the national risk assessments have not yet had any direct impact on the practices of the criminal prosecution authorities, the police have for some time taken risk into account: the Department for Economic and Financial Crime has adopted a programme package *Recovering Illegally-acquired Assets and Money Laundering*. It advocates a targeted approach to ML, concentrating police resources on the groups of perpetrators judged as priority when it detects either suspect assets held by legal persons, or the use of cash for ML purposes. Similarly, a Federal Police Service specifically for diamonds was set up in Antwerp in 1998. Lastly, the Federal Police's Central Service for Terrorism and Sects uses measures against terrorist financing to destabilise terrorist groups as part of the 'destabilisation' section of its terrorist and extremist violence programme. The systematic inclusion of ML/TF risks in the work of the courts has not been observed, although there have been some isolated initiatives (for instance, one court has developed a means of targeting people with a lifestyle evidently more lavish than their declared income) (see Section 3).

2.30. **Supervisors have not in general included the principal threats and vulnerabilities identified by the national risk assessments in their supervisory policies.** Although its resources are limited, FPS Economy seems to have fully recognised the threats linked to the diamond sector and the issues raised by cash. The FSMA and the BNB have identified the main activities under their control that are exposed to ML/TF risks (see Section 6). In their circulars to the financial institutions,⁵ they draw attention to particular risk criteria and recently issued a warning concerning the risks related to the activity of gold recycling. Nevertheless, in their supervisory work the authorities have not yet focused more of their effort on auditing the implementation of preventive measures for customers most at risk of laundering money from tax fraud, or on business relationships with professions that the national risk assessment judged to be sensitive, such as diamond traders, lawyers and retailers who handle significant amounts of cash. AML/CFT is still not sufficiently considered when defining the risk profiles of entities undergoing inspections, which would then be used to determine the frequency and scope of such inspections.

2.31. **The reservations expressed by the accountancy and legal professions, lawyers in particular, about the national risk assessments are problematic.** The supervisory bodies for these professions did not provide a contribution to the national ML risk assessment, and although they say that they started to consider risk once they became aware of these analyses, they do not share the assessment's conclusions, which present their professions as particularly risky in terms of ML. They consider that they have adequate controls in place to counter the main threats and that misconduct is largely the preserve of those outside the regulated professions. With the exception of one analysis carried out by the professional association of diamond traders that noted an absence of major risks in the sector, no sectoral assessment (by the supervisors of the sectors themselves) had been finalised as at the date of the on-site visit, despite current initiatives.⁶

(e) The co-operation and co-ordination of the competent authorities and the self-regulatory bodies

2.32. **In general, the framework for AML co-operation and co-ordination appears adequate.** A large number of the competent authorities are already members of the College for combatting tax and welfare fraud,⁷ created in 2008, and these authorities follow an annual action plan. Creating a co-ordination body that covers AML and its various structures is progress towards better co-ordination and co-operation between

5 CBFA Circulars dated 6 April 2010 and 1 March 2011, BNB/FSMA Circular Recent developments in the prevention of money laundering, (BNB/FSMA, 2013).

6 The accountancy profession, the financial sector and lawyers have indicated that they are working on an ML/TF risk assessment for their respective sectors.

7 Its members are senior officers from the social services and tax authorities, the judiciary, the police services involved in combating tax and welfare fraud, and the CTIF.

the competent authorities and the supervisors. The development should encourage greater co-ordination between the CTIF and the financial supervisors. This co-ordination already exists as regards policies, but is insufficient as regards prevention activity. For instance, there is no structured information exchange to target inspections, apart from isolated communications made by the CTIF (Art. 35 of the AML/CFT Law) which feed into the analysis of the risks associated with the financial institution concerned. Discussions are nevertheless in progress to formalise and strengthen the relationship between the CTIF and the BNB. Co-ordination is evident also in the joint circulars prepared by the FSMA and the BNB, on the compliance function in December 2012 and on recent developments in ML prevention in December 2013. The Federal Police also encourage co-ordination on AML/CFT questions with the CTIF and the College of Procurers-General, in order to prepare the National Security Plan. Neither supervisors for the accounting/tax and legal professions and gambling or the intelligence community seem to be sufficiently involved. There is also no operational co-operation between the CTIF and the supervisors (for instance, to report members of the professions who should undergo AML/CFT inspections, as permitted under Art. 35 of the AML/CFT Law).

2.33. **The framework for TF/PF co-operation and co-ordination has been developed** but suffers because key administrative authorities for TF/PF within the CRS (the CTIF and supervisors) are not represented. The Federal Police also encourages co-ordination on TF questions with the CTIF and the College of Procurer-Generals, in order to prepare the National Security Plan. The TF Unit of the Central Service for terrorism and sects also exchanges information with AGDA about the problem of cross-border cash flows, the intelligence services, the CTIF, and OCAM.

2.34. **As regards combatting proliferation, including financing of proliferation, FPS Foreign Affairs holds interdepartmental co-ordination meetings** relating to the implementation of UN sanctions or EU restrictive measures, attended by the National Security Service. The National Security Service is also in direct contact with the Treasury administration, which is responsible for reviewing the financial aspects of transactions between Belgian and Iranian businesses. The Regional Services controlling exports of dual-use items act generally as a front office for files they submit for opinion to the multidisciplinary Advisory Commission on the Non-proliferation of Nuclear Weapons. Since the Iranian transport sector (maritime and air) is subject to sanctions, FPS Mobility & Transport and FPS Interior are also involved. Lastly the administrations responsible for export control, AGDA and FPS Foreign Affairs have established formal procedures for co-operation in order to monitor exported goods. Nevertheless, the absence of a formal mechanism linking the CTIF and the supervisors of financial institutions and DNFBPs to the CRS limits the scope for co-ordination and co-operation in relation to TF/PF, although this is mitigated, for the CTIF in any case, by its contribution to the national TF risk assessment.

(f) Informing financial institutions and designated non-financial businesses and professions (DNFBP) of the results of risk assessments

2.35. The professional associations of the financial institutions and DNFBPs were notified in June 2014 about the national ML risk assessment of December 2013. **At the time of the on-site visit, the financial institution and DNFBP representatives met with generally were not aware of the national ML/TF risk assessments.**⁸ A presentation was made to accountancy professionals in February 2014 and to the FEBELFIN, the Belgian financial-sector Federation, in July 2014. There had been no other briefing or guidance on the conclusions from the risk assessments, either in general or specific to the sectors concerned as at the time of the on-site visit. In particular, there will be further discussions with the legal and accounting/tax professions that have expressed reservations about the assessment (see above). There had been no communication on the national ML risk assessment, which poses a particular problem regarding the low level of understanding by NPOs of TF risks.

2.36. **However, information on the ML/TF risks has long been communicated to the financial institutions and the DNFBPs.** The CTIF raises the awareness of the private sector and the relevant authorities to the risks of ML and TF by publishing warnings and typological analyses on its web site. The financial sector

8 The authorities provided information to the evaluators leading them to believe that in autumn 2014 financial institutions and DNFBPs had knowledge of the ML risk assessment.

supervisory guidelines of 2010/11 and the joint FSMA/BNB circular of December 2013 on cash in the gold sector (referred to above) are also a means of providing information on the risks. As regards TF risks, a memorandum of understanding between FPS Justice and FPS Interior and the Federation of Enterprises in Belgium has been in place since 2009, on the mutual exchange of information relating to signs of a possible terrorist threat, which includes terrorist financing.

2.37. ***In conclusion***, Belgium assesses its ML and TF risks. It appears to understand the TF risks correctly and has taken co-ordinated steps to mitigate those risks at the national level. This co-ordination also addresses combatting the financing of proliferation. While ML risks appear to be identified and understood overall, the analysis of this activity is not approached proactively so as to enable the identification of trends or emerging phenomena, notably with regard to vulnerabilities. In particular, the assessments did not benefit from the contribution of all competent authorities or the private sector. Elements of a risk-based approach have for many years fed into the development of AML policies and activities. The CTIF, and to a large extent the law enforcement authorities (especially the police) have traditionally considered the identified risks when defining their objectives and activities. Nevertheless, a certain number of weaknesses were noted at the time of the on-site visit:

- i. there is no overall, integrated approach that adequately ranks ML/TF risks in order to ensure the organisation and consistent planning of AML/CFT activities and policies;
- ii. supervisors and self-regulatory bodies (SRBs) have not incorporated the main ML/TF risks into their inspection policies;
- iii. a certain number of identified ML risks have not been addressed; and
- iv. incomplete dissemination of the non-confidential results of the risk assessments to financial institutions and DNFBPs slows down their being taken into account in their internal procedures.

2.38. **Belgium has achieved a substantial level of effectiveness for Immediate Outcome 1.**

2.4 Recommendations on National AML/CFT Policies and Co-ordination

2.39. The following important measures appear necessary to improve the understanding of risks and their being taken into account in national policies and co-ordination.

- The ML risk assessment should be strengthened by the inclusion of (i) additional elements on threat including from the intelligence services, in confidential sections if necessary; (ii) information on vulnerabilities provided by the supervisors of financial institutions and DNFBPs or derived from statistical sources (for example, STATBEL, EUROSTAT, BNB and ECB); and (iii) contributions from the private sector.
- The understanding of TF risks will be supplemented by an increased participation of the CTIF in the work of the CRS and by creating mechanisms that associate the competent supervisory authorities.
- Belgium should seek to implement policies that address the recommendations of the ML risk assessment, particularly regarding resources for the justice system and the effectiveness of inspections and administrative sanctions.
- Exceptions to CDD measures should be supported by the findings of the national risk assessments.
- Supervisors should incorporate knowledge of the main threats and vulnerabilities identified by the national risk assessments into their supervisory policy.

- The non-confidential findings of the national risk assessments, along with their future updates, should be communicated in a timely manner to the institutions and persons subject to the AML/CFT Law and to the other sectors concerned (such as NPOs).

2

Bibliography

BNB/FSMA (2013), *Evolutions récentes relatives à la prévention du blanchiment de capitaux*, Circular Recent developments in the prevention of money laundering, BNB/FSMA, December 2013, www.nbb.be/doc/cp/fr/ki/circ/pdf/nbb_2013_16.pdf

FATF and Egmont Group (2014), *Money laundering and terrorist financing through trade in diamonds*, FATF, Paris, www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-through-trade-in-diamonds.html



3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings

The Belgian law enforcement authorities have ample powers and an adequate legal framework. However, structural problems prevent them from being fully effective; the Belgian judicial authorities have insufficient human and technological resources, and this has an impact on AML activities.

Use of Financial Intelligence

- The CTIF is a financial intelligence unit (FIU) with broad access to useful AML information which it exploits systematically. The CTIF produces high quality operational and strategic analyses. Its reports contain financial information and important analyses that are able to trigger criminal investigations into ML/TF.
- The law enforcement authorities have a wide variety of measures available for their investigations. These can be used to obtain all the information necessary for seizing assets and identifying the perpetrators of offences with a view to their prosecution. However, they do not make the most effective use of all the data placed at their disposal because of a lack of resources.

AML Strategy of the Prosecution authorities

- The general level of awareness, knowledge, and understanding of ML risks for the Belgian judicial authorities is good. However, at national level the prosecution authorities have no clearly defined overall strategy for combatting ML. Nor is there co-ordination between judges at national level as regards the prioritisation of prosecutions.
- Offences and their perpetrators which are reported to prosecution authorities are based in part on STRs, mainly submitted by credit institutions, but also by foreign FIUs. Other ML cases are detected mainly by the police, customs, the tax authorities and through the investigation of predicate offences.
- The number of STRs coming from certain of the obligated non-financial sectors (particularly lawyers and diamond traders) does not seem commensurate with the identified risks. Some ML offences therefore seem to evade prosecution through a failure to detect them. The possibility of seizure or confiscation of property is an important factor in determining whether a criminal investigation will be initiated. Prosecutions are primarily oriented towards predicate offences, particularly fraud, offences related to bankruptcy, tax fraud and narcotics trafficking. In these contexts, ML prosecutions are principally oriented towards the perpetrator of the predicate offence ('self-laundering'); cases of third-party ML are less common.
- If prosecution for the predicate offence is not possible, this does not in practice prevent prosecution for ML as a standalone offence, particularly in cases of cross-border transportation of currency.

3

- The system for detecting cross-border currency movements works well in Belgium, but the declarations/disclosures stemming from it are not subject to follow-up, prosecution, or confiscation in proportion to the level of risk cited by the competent authorities. The low priority given to these cases is linked to a lack of human resources within the public prosecutor's office.

Criminal Sanctions

- The sanctions regime is satisfactory. However, the law enforcement authorities' lack of resources slows down proceedings, significantly reducing the effectiveness and deterrent effect of sanctions, because the length of the proceedings affects the length of sentences handed down by the court. The [failure to meet the] statute of limitations for offences and proceedings leads to the risk that no conviction will be handed down. The success rate for ML in big cases, particularly for international cases, is low, most notably because of difficulties related to international co-operation and the lack of resources.
- The legal framework for prosecuting legal persons poses problems as regards application. Moreover, because complex ML cases are uncommon and proceedings focussed on the physical persons, convictions are limited as a result.

3.1 Background and Context

3.1. The legal basis for the criminalisation of ML in Belgium has, since 1990, been set out in Art. 505 PC. The law was judged compliant with FATF standards during the last mutual evaluation. However, the Belgian parliament has since amended Art. 505 to make the Article's scope more specific and thus improve its effectiveness and legal certainty (Law of 10 May 2007¹).

3.2. All crimes (*crimes et délits*) under Belgian law may be predicate offences for ML (including serious tax fraud offences, whether or not organised). Because ML covers the laundering of assets that are the proceeds of any offence, all the designated categories of offences defined by FATF are covered.

3.3. Art. 42ff. PC establishes the legal basis for the confiscation of the instrumentalities and proceeds of offences. These measures can be applied to all crimes (*crimes et délits*), including ML and TF. Since amendment of the law in 2007, it has been possible to order confiscation in respect of all perpetrators, co-perpetrators or accomplices in ML cases, even if the person convicted is not the owner of the assets to be confiscated (this closed a loophole concerning confiscation of a corresponding value). The 2007 amendment PC was also designed to close a loophole concerning criminal seizures.

3.4. ML investigations and prosecutions are led by the public prosecutor's office, which can refer more complex cases and cases requiring special investigative powers to an investigating judge (*juge d'instruction*). The public prosecutor's office and investigating judges receive assistance from the judicial police and contributions from CTIF. Cases are then judged by courts of first instance (for less serious crimes [*délits*]; and by assize courts for more serious crimes [*crimes*]), appeals go before appeal courts, and the parties to a case can refer the case to the court of final appeal (*Cour de cassation*) (to rule on points of law rather than to appeal again on the merits of the case).

3.2 Technical Compliance (R.3, R.4, R.29-32)

Money Laundering and Confiscation

Recommendation 3 – ML Offence

3.5. **Belgium is compliant with R 3** – The criminalisation of ML (Art. 505 PC) lists the elements constituting the offence of ML as defined in the Vienna and Palermo Conventions. According to consistent case-law (and the spirit of the law), prosecution for ML is not dependent upon conviction for the predicate offence. All legal persons are criminally liable for ML offences linked to accomplishing the purpose for which they were created or the defence of their interests, or that are committed on their behalf.

Recommendation 4 – Confiscation and provisional measures

3.6. **Belgium is compliant with R 4** – Belgium has a comprehensive legislative framework for seizure and confiscation. Art. 42ff. PC defines a special regime for confiscation (as an ancillary order to a main sentence); confiscation is thus linked to a criminal conviction. Various types of provisional measures aimed at blocking transactions involving property that could be subject to confiscation are available in Belgium. Seizure allows property, instrumentalities, and proceeds of crime and financial benefits arising directly from offences to be withheld. This is complemented by freezing measures that are available to administrative authorities (including CTIF).

1 For an explanation of the reasons for this change, see the draft law of 11 February 2005 (51-1603/001).

Operational and Law Enforcement Authorities

Recommendation 29 – Financial intelligence units

3.7. **Belgium is compliant with R 29** – Belgium’s FIU, the CTIF, is an independent and autonomous authority responsible for the processing and disseminating of information linked to AML/CFT, and for analysing information received in the context of ML investigations, the associated predicate offences and TF (AML/CFT Law).

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

3.8. **Belgium is compliant with R 30** – Belgium’s law enforcement authorities are responsible for leading and carrying out investigations into ML, predicate offences, and TF. These tasks are shared between the Federal Prosecutor’s Office, the regional prosecutor’s offices, investigating judges and the judicial police.

Recommendation 31 – Powers of law enforcement and investigative authorities

3.9. **Belgium is compliant with R 31** – Law enforcement authorities have all the classic investigative methods as laid down by the Code of Criminal Procedure (CCP) available to them for AML/CFT operations and for the investigation of the predicate offences. These authorities are in particular able to obtain banking information linked to natural and legal persons.

Recommendation 32 – Cash couriers

3.10. **Belgium is compliant with R 32** – Control of cross-border movements of currency and bearer negotiable instruments relies on a dual regulatory system (Reg. 1889/2005 and RD of 26 January 2014 (national)). It consists of a *declaration* system (for money movements into, or out of, the EU) and a system of *disclosure* on request (for money movements within the EU).

3.3 Effectiveness: Immediate Outcome 6 (Financial Intelligence)

3.11. The Belgian authorities have access to a wide variety of financial and other intelligence, particularly tax-related, which is useful and necessary for investigating ML, the predicate offences and TF. This information is contained mainly in public records such as the land registry and the BCE (the register of information on all legal persons under Belgian law, see Section 7) and is supplemented by exchanges between relevant authorities (see point d). Searching for and using this intelligence is common practice of the Belgian authorities, particularly of the CTIF and the law enforcement authorities. The assessors noted a variety of examples of this, confirming access to and use of this information for ML and TF investigations.

(a) Access to and use of financial intelligence and other relevant information

3.12. **The CTIF has overall effective access to financial intelligence and a large amount of other information**, particularly tax-related, which it needs for analyses and for preparing its reports, through contacts established with all public authorities (particularly the police and judicial authorities, SE, SGRS, the tax authorities, and the National Social Security Office). Not only does it receive a large amount of unsolicited intelligence, but it also requests and obtains intelligence it needs. Furthermore, memoranda of understanding (MOUs) have been signed between the CTIF, SE and the SGRS in order to ensure good information exchange among them. The CTIF is also able to supplement this information by sending queries to the financial sector and DNFBPs, as well as foreign counterparts. Research and entering information into the police database is facilitated by the secondment of a Federal Police liaison officer to CTIF. The names of persons appearing in suspicious transactions are systematically checked against the population register, national criminal records, the BCE and the CTIF database. They are also systematically checked against police databases. In cases of suspicions linked to serious tax fraud offences or to violations of laws under the responsibility of AGDA, following the transmission of the file to the prosecutor’s office, the CTIF provides to SPF Finance (CAF)

relevant information resulting from the submission of the file to the prosecutor. CTIF's research is facilitated by the secondment of liaison officers to CTIF from the tax authorities.

3.13. During the 2009-2013 period, CTIF disseminated 6 298 case files on potential ML or TF transactions worth a total of EUR 8.4 billion (these cases were based on 25 979 suspicious transaction reports, with some cases linked to more than one STR). **In 2012, 75% of case files on ML as an indicator of a predicate offence came from CTIF.** The remaining 25% came from investigations by the police, the tax authorities, crime reports, etc. Nearly half of all case files sent to the public prosecutor's office are not followed up with police or judicial investigations (*informations judiciaires ou instructions*) for reasons of expediency, or for technical reasons (see IO 7). This results from the fact that the CTIF is obliged to transmit all serious suspicions of ML, regardless of how important the offence is, while the public prosecutor has the discretion to open a case or not. CTIF is nonetheless an important source of information justifying the initiation of ML proceedings. The crimes pursued through the courts are as a general rule the predicate offences identified by CTIF (fraud, fraud linked to bankruptcy, illegal drug or goods trafficking and serious tax fraud).

3.14. When CTIF notices in a case file it is sending to the judicial authorities that large sums could still be seized, it immediately notifies the OCSC (see IO 8). Between 2009 and 2012, CTIF sent 284 such notifications to the OCSC; in 2013 it sent 83.

3.15. Law enforcement authorities have available and use a wide range of financial research measures in their investigations of ML, predicate offences, and TF. In practice this research consists of establishing and consolidating the reported facts, and identifying and tracing the assets related to the offences, including any held abroad. The authorities can also do all this research through international mutual legal assistance (see Section 8). They also have a privileged access to the BCE. Criminal prosecution authorities work closely with the police, who also have a broad access to records and databases.

3.16. In order to reinforce the investigations of the prosecutors (RD of 21 January 2007) and the police (RD of 23 January 2007), employees of the tax authorities are seconded to and work with these authorities so as to assist in combatting ML, as well as economic and financial crime. These tax assistants, who operate independently of their home agency, have the status of expert-assistant to the prosecutor or officer of the judicial police. Their tasks consist of providing assistance in criminal proceedings, in particular regarding contacts with the tax authorities. There is a particular focus on tax in criminal investigations of ML.

3.17. **In regard to obtaining banking information**, according to the Public Prosecutor, for the years 2010 to 2012, the number of information requests to banks relating to all offences came to approximately 2 300 per year, and the number of requests to freeze bank accounts came to about 170 per year (with an upward trend of 50% per year). It is impossible to know the number of these requests that are related to ML, but this information indicates at any rate that requests are made directly to banks and that the institutions comply with the requests. There are no statistics for investigating judges; however, one of the investigating judges interviewed during the on-site visit indicated that he made requests for banking information on a daily basis. Prosecutors and the police use a system called FUSE for transmitting their requests to all credit institutions in Belgium. According to information provided by Belgian authorities, this system was used just under 2 000 times per year in the totality of investigations conducted by law enforcement.

3.18. It is difficult to know the extent to which the authorities find and use all the financial intelligence and other information available for investigations of ML and TF and for tracing assets that could be confiscated. The statistics and data are inadequate. For example, there are no statistics available concerning financial and asset investigations solely for the ML offence (see TC Annex, R.33). The database held by the public prosecutor's office does not make the internal exchange of information between the law enforcement authorities very easy, mainly because of an inadequate IT system and imprecise input criteria.

3.19. Nor do the data provided by the Belgian authorities reveal the extent to which the law enforcement authorities seek financial information from abroad in the context of mutual legal assistance, to provide further evidence in proceedings concerning ML and TF (see Section 8).

3.20. The information provided nevertheless tends to show that, in criminal prosecutions, **the available information and databases are not searched and used in the most effective way.** The Public Prosecutor

explained that the complexity of ML cases often requires using a number of investigative actions such as international rogatory commissions, banking investigations, asset tracing or technical investigations such as wiretapping. It follows that long and costly investigations therefore need to have both specialised judges and investigators, and this can have an impact on investigative capacity in this area.

3.21. One investigating judge indicated that he only carried out full **asset investigations on rare occasions** because they took up significant amounts of investigators’ time, which was a problem given the shortage of manpower, so the tendency was to focus on assets that were readily available (see IO 7). However, in a number of cases it seemed that investigators had managed to trace back along a series of transactions and locate the proceeds of offences, and investments made using these proceeds, including abroad (e.g. ruling of the Final Court of Appeal [*Cassation*], 17 December 2013). The research was often more detailed when there were victims to be compensated (e.g. in the case of ML linked to fraud).

3.22. The CTIF noted that during the past few years, several large cases had been transmitted to the judicial authorities and dealing with significant amounts of ML. However, the cases did not end successfully because the acts fell beyond the statute of limitations and violated rules on reasonable delay. To this should be added that a not insignificant number of cases were simply closed on expediency (*principle of opportunity*). **This finding reinforces the conclusion that the use of financial information by judicial authorities is not done systematically or appropriately** (even if this shortcoming is not the only one that would explain the problem with delays, see IO 7).

(b) Types of Reports Received

3.23. **CTIF acts as a central agency for receiving communications from the reporting entities concerning ML and TF and as a filter between these reporting agencies and the judicial authorities.** Reports are issued by many entities, particularly in the financial sector and the designated non-financial professions (see table in Section 5), as well as many State agencies, particularly the police (for a detailed analysis of relations between CTIF and the financial institutions and designated non-financial businesses and professions, see Section 5.3).

Table 3.1. Suspicious Transaction Reports (STRs) and Cases

	2009	2010	2011	2012	2013
Number of STRs received	17 170	18 673	20 001	21 000	22 966
Number of new cases	3 201	3 220	3 323	4 002	5 063

Source: CTIF

3.24. While the number of STRs received is large, not all of the STRs have the same importance or require the same amount of attention. Thus 30% of STRs are based on ‘subjective’ criteria (suspicion), while 70% are based on ‘objective’ or automatic criteria (exceeding thresholds: e.g. RD of 1999 for casinos; Art.20 of the AML/CFT Law for real estate transactions; Art.21 for limitations on payments in cash). This latter category requires less analysis. The financial sector has generally accepted the practice of reporting suspicious transactions (STRs), which are overall of a high standard, clear and complete, thus permitting analysis of suspicious transactions. In the money exchange sector and, to a certain degree, for money transmitters, a practice of ‘defensive’ or automatic STRs was noted. These are not supplemental or follow-up STRs and are submitted automatically and without any suspicion for any new transactions carried out by a customer who has already been the subject of one or more STRs (see Section 5). To deal with the number of STRs and process them efficiently, the CTIF has, through its strategic analysis department, put into place a tool that identifies suspicious transactions and determines priorities. ML indicators are studied whilst taking into account identified criminal phenomena, modus operandi, frequency, and links to data recorded in the CTIF database. As well, the CTIF has contact with the reporting institutions, in particular to request supplemental information for analysis and processing of STRs. To improve the quality of STRs, the CTIF issued guidelines in December 2013 (also available on the CTIF website) that enable reporting institutions to fill in a standard STR form, which contains all elements needed by CTIF to conduct its analysis. Furthermore, based on the first

national ML risk analysis, **the CTIF developed in 2014 a risk-based approach** to the operational processing of ML cases based on STRs.

3.25. Since January 2010 CTIF has been able to receive STRs from the Federal Public Prosecutor's Office in the context of police or judicial investigations into TF, and from the European Anti-Fraud Office (OLAF) where there is a suspicion of fraud against the financial interests of the EU. This capacity was extended in March 2012 to officials working in State administrative agencies, where there is a suspicion of ML and TF. Based on this information, public authorities appear to be increasingly inclined to report suspected ML to CTIF. This is shown by the following table, even though it would be expected to see more reporting from enforcement authorities (police and public prosecutors) (see also the discussion of the lack of feedback from the public prosecutor's offices to CTIF above). As an example, FPS Finance drafted an internal circular to raise the awareness of its officials on the subject in October 2014 and to specify the various practical means of transmitting information between CTIF and FPS Finance.

Table 3.2. Spontaneous Reporting to CTIF by the Public Authorities

	2009	2010	2011	2012	2013	Total
Police	10	11	17	49	41	128
Judicial authorities – public prosecutors	5	3	6	5	13	32
State administrative agencies	14	17	30	7	14	82
Officials in State administrative agencies	-	-	-	31	66	97
Federal prosecutor's office (TF)	-	0	0	0	0	0
OLAF (fraud against the financial interests of the EU)	-	0	0	0	0	0
TOTAL						339

Source: CTIF

3.26. All information relating to cross-border cash movements is automatically sent to the central information management service of AGDA. This service forwards it to CTIF, which processes the information. Reports, drawn up if ML or TF offences are committed or suspected, are sent to the public prosecutor's office and to CTIF.

(c) FIU Analysis and Dissemination

3.27. **CTIF has an analysis department** with 25 to 30 staff, which has adequate human and material resources, and uses all the powers at its disposal to analyse and enrich the information it receives on reported transactions and facts, for the purposes of both prosecuting for offences and identifying and tracing assets that could be confiscated.

3.28. **CTIF manages its own databases for all intelligence received.** Although it enjoys extensive access to other databases for the purpose of adding information to its reports, CTIF cannot however access the register held by the BNB giving the identities of bank customers and their account numbers (register created by the Law of 14 April 2011). It therefore has to send requests to every bank operating in Belgium's financial sector when it needs details concerning a bank account, which is an onerous process for both the banks and CTIF and can pose problems as regards data protection.

3.29. If there is a sufficient level of suspicion, CTIF sends to the prosecution authorities an analytical report containing:

- the details of the persons concerned,
- a detailed description of the suspicious transactions, intelligence concerning the previous police records of the persons concerned (from the federal and local police), and

3

- intelligence gathered from various other public authorities (tax, social security, etc.) where appropriate,
- information obtained from the intelligence services,
- any publicly available information (from the internet) and
- a description of the ML or TF indicators.
- Identity documents, bank account application documents, account histories and supporting documents are sent with the reports.

3.30. Over the last five years (2009 to 2013), around 40% of reports based on suspicions of ML/TF (i.e. based on 'subjective' criteria) received by the CTIF were transmitted to judicial authorities, and 25% of reports based on fixed criteria or thresholds (i.e. 'objective' or 'automatic') were submitted. In spite of the number of files opened by CTIF, the number of files transmitted to judicial authorities went down in 2013, since the increase in suspicious reports occurred in the last months of 2013.

3.31. In the context of dissemination of its reports and to meet the requirement for confidentiality, CTIF works with many partners not only to add to its own information but also to strengthen action to combat ML and the predicate offences (in particularly the federal judicial police, local police, judicial authorities, tax authorities, intelligence services [SE, SGRS], National Social Security Office and customs [AGDA]). So for example, between the end of 2009 and the end of 2013, some 827 items of information from CTIF were received by the Anti-Fraud Co-ordination Service (CAF) at FPS Finance. This information enabled tax corrections to be made for this period worth a total of EUR 157 million.

3.32. **The reports and analyses produced by CTIF meet the operational needs and expectations of the competent authorities.** The prosecutors and judges met by the assessors feel that these reports and analyses are of a high standard, enable proceedings to be initiated, and point investigations in the right direction.

3.33. The average time taken by CTIF to process suspicious transaction reports and send a report to the prosecution authorities is approximately three months. All the authorities concerned feel that this is a reasonable amount of time.

3.34. Since 2009, CTIF has had its own strategic analysis department (with around four staff) which helps to provide a better understanding of ML/TF trends and to put the indicators and suspicions reported by the reporting entities into context. In particular CTIF keeps statistics, which it uses as the basis for the analyses it publishes, for example, in its annual reports, based on its own information, as well as on exchanges with other public authorities. CTIF provides training to its staff and participates in other training, for example, for the financial and insurance sectors.

3.35. **This type of analysis also enables CTIF to play a preventive awareness-raising role**, particularly by sending out information and indicators concerning suspicious financial transactions to the sectors concerned (e.g. on VAT carousels). It publishes and updates the guidelines to be used by the organisations and professions covered by the AML/CFT system. On its website (www.ctif-cfi.be), it disseminates typologies information and analyses. A number of strategic analyses (around 38 since 2009) have been produced for the authorities and reporting entities (e.g. *Money Laundering and the Use of Limited Companies, The Proliferation of Weapons of Mass Destruction, Terrorist Financing – Yemen, Money Laundering and Football*). CTIF also regularly takes part in working groups, in fields that could be useful for gathering further information to enrich its operational analyses (e.g. the CTIF/State Security working group on proliferation, Working group on the diamond trade and Working group on fraud in sport (*Transparency International, Brussels*)).

(d) Co-operation and exchange of information

3.36. As indicated above, the CTIF works with a number of public authorities in its work to gather and analyse information.

3.37. To carry out judicial investigations (*informations judiciaires*), **prosecutors and investigating judges** make requests to police, tax authorities, the BCE, banks, etc. For ML cases, the number averages 4 200 requests per year for the last eight years (not including the requests made by investigating judges, who are responsible for the largest ML cases). In this context, the judicial police also have access to a number of databases and work with various government agencies and foreign colleagues. The police generally have sufficient resources to carry out its mission.

3.38. Nevertheless, **the relations and the dialogue between the CTIF and the prosecution authorities should be reinforced, particularly in operational cases.** Although the CTIF and the public prosecutor's office meet regularly to discuss typologies (e.g. in 2011 there was a meeting with the Federal Prosecutor's Office on fraud via the internet), as well as terrorism and TF, co-operation on specific ML cases is poor. The public prosecutor's office has access to part of CTIF's database (concerning the files transmitted) through the judge points of contact, but little use has been made of this access (the database has been consulted 54 times since 2010). Apart from the legal obligation to inform CTIF of final decisions in cases originating with suspicious transaction reports (an obligation that is not always observed), the public prosecutor's office passes on little information to CTIF spontaneously about the follow-up given to its reports, particularly concerning asset freezing. Because final decisions in ML cases can come years after the facts were originally reported, the added value of receiving this information is diminished. CTIF and the public prosecutor's office both agree that the contact between the two has long been insufficient. Horizontal co-operation needs to be improved generally: It is important that CTIF receive feedback from the prosecution authorities on the initiation of any proceedings and on any asset seizures made, well before the final court judgment. CTIF may request this information on a case-by-case basis consistent with the needs of a case through the liaison officers of the Federal Police seconded to CTIF. However, without regular and appropriate feedback, it is more difficult for CTIF to do an effective job of analysing new evidence, which could be compared with cases already sent to the public prosecutor's office. Some improvements have recently been made (in October 2013) so that cases opened on the basis of information supplied by CTIF are identified as such, and this should increase the amount of feedback given.

3.39. **Likewise, the relationship between CTIF and the OCSC could also be strengthened.** CTIF, which examines STRs and knows of the assets that could be involved in ML or predicate offences, **does not have direct access to the OCSC database** and must make requests for such information as needed. Knowledge, in a timely manner, of a possible link between assets entered in the database and the suspect assets about which it receives information could improve tracing of assets with a view to their confiscation. The Belgian authorities indicated that, besides the ability to request information from the OCSC on specific cases, the CTIF and the OCSC both have liaison officers assigned to the Federal Police, who meet annually to exchange information on the seizures that have taken place in relation to urgent CTIF cases (2- to 5-day freezes, cases with significant amount of money to freeze). There as well, the communication of information on a case-by-case basis does not provide for optimal conduct of asset tracing, given the dynamic of seizures and confiscation. During the on-site visit, it was found that the various authorities had no common viewpoint on the number and amounts of seizures and confiscations, in particular among the OCSC, the CTIF, the public prosecutors and the investigating judges. This means that financial information is not optimally sought out and exploited.

3.40. **CTIF is working on an action plan** that would establish a monitoring system, and on strengthening co-ordination between the various partners in the fight against ML, TF and their prevention.

3.41. The figures given in Table 3.3 below show the number of requests made by CTIF to the reporting entities in the context of its analyses (not counting the databases to which CTIF has direct access).

3.42. **The CTIF is particularly careful in practice to protect the confidentiality** of the financial and other intelligence it gathers, and an IT security policy has been drawn up. CTIF's offices, where the STRs are processed and which can initiate requests and communications with other authorities, are also separate from other agencies. Exchanges of intelligence with foreign FIUs also take place across secure networks, FIU.NET

and Egmont Secure Web.² However, it should be pointed out that CTIF’s reports are not sent to the public prosecutor’s office via dedicated channels (they are generally sent by courier or registered post).

Table 3.3. Sources of information

Public authority	2010	2011	2012	2013	Total
Foreign counterparts	2 457	1 376*	1 639	1 319	6 791
Tax authorities	211	337	328	317	1193
FPS Social Security	157	299	272	248	976
State Security	73	116	105	118	412
Fraud pattern monitoring centre	91	76	74	51	292
SGRS	56	82	53	62	253
OCAM	18	47	35	47	147
OLAF	14	16	18	13	61
National Employment Office		2		1	3

Source: CTIF

* Until 2010, intelligence requests sent via FIU.NET (between EU FIUs) were counted in terms of the number of people involved. Since 2011, the requests submitted have been counted in terms of the number of cases (there can be several people involved in a single case).

3.43. **Regarding international co-operation, CTIF has extensive mutual assistance relationships** with its foreign counterparts (see above table on CTIF’s sources of information; CTIF also receives 450 requests per year on average). The FIU’s co-operation with its foreign counterparts appears to be adequate and effective (see Section 8).

3.44. **In conclusion, Belgium’s legislative framework provides the competent authorities with a very broad selection of measures for searching for financial intelligence** and any other relevant information in the context of ML/TF investigations, for the purpose of both demonstrating that offences have been committed and for tracing the associated assets.

3.45. **The CTIF gathers a large amount of information on ML and TF**, and its research is of a high standard. CTIF uses a large number of databases and maintains co-operative relationships with any national and international authority capable of contributing or adding value to its work. CTIF also performs vulnerability analyses of the sectors covered by the law, and these are sent to all the authorities and persons concerned. Its reports are appreciated and found to be useful by law enforcement authorities.

3.46. Law enforcement authorities make use of and research information, both to initiate an investigation and to carry out proceedings; however, they do not do so in an optimal manner. Limited human resources do not allow prosecution authorities to use the information received correctly or to fill in the gaps so as to reveal ML cases, particularly large ones or those with international implications.

3.47. **Belgium has achieved a substantial level of effectiveness for Immediate Outcome 6.**

2 FIU.NET is a decentralised computer network that assists EU FIUs in their efforts to combat ML/FT. The system is decentralised in the sense that there is no central database where all the exchanges are recorded. When intelligence is sent from one FIU to another, it is stored securely but only in the FIU.NET databases of the parties involved. Egmont Secure Web is a secure internet system that allows members of the Egmont Group to communicate with one another using a secure electronic messaging service and to request and share information about cases, patterns, analysis tools, etc.

3.4 Effectiveness: Immediate Outcome 7 (ML Investigation and Prosecution)

3.48. ML investigations are carried out by the **Belgian public prosecutor's office and the investigating judges**, and prosecutions by the public prosecutor's office. The legislative framework places a broad range of investigative measures at their disposal, enabling them to carry out detailed investigations so that all those involved in offences (perpetrators, co-perpetrators, accomplices, etc.) can be prosecuted (see TC Annex, R 30 and R 31). Investigations can be opened by an investigating judge once a pre-trial investigation has been ordered, since judges have greater enforcement powers at their disposal: 100 ML cases on average are subject to judicial investigation every year.

3.49. **The public prosecutor's office and investigating judges are responsible for prosecutions of offences.**

3.50. The public prosecutor's office and investigating judges can seek assistance with conducting proceedings from the **Federal Judicial Police** (in big cases) and the other police services. They have the power to investigate multiple aspects of offences (administrative, tax, etc.). The federal police also carry out ML detection, for example by detecting and intercepting currency movements (Cash Watch³) or as part of a project to detect suspicious capital increases in the context of the involvement of legal persons in ML schemes (see Section 7). The police also have a special section dealing with the diamond trade.

3.51. The ML offence is well accepted by Belgian law enforcement: it is frequently prosecuted, particularly in association with economic offences that generate significant profits to be traced because they facilitate confiscation (fraud, offences linked bankruptcy, benefits and tax fraud), especially in cases of self-laundering.

(a) Launch of investigations and prosecutions

3.52. **In practice it is mainly the public prosecutor's offices in Brussels and Antwerp that handle major ML cases** (by way of an indication, these Offices receive around 37% and 15% respectively of STRs submitted by CTIF).⁴ Although the other public prosecutor's offices also handle ML cases, there is no consensus among the different offices and investigating authorities as to the criteria for launching and conducting an investigation. The Brussels public prosecutor's office, which has a very large workload, has set criteria (below) to focus the available investigative means on certain cases so as to avoid the dispersal of its resources. The information and statistics provided by the public prosecutor's office tend to show nonetheless that the prosecution authorities have a very large workload.

3.53. **There is no general criminal policy guidance for AML action** covering the whole of Belgium, which would allow clear priorities to be set for ML investigations. Nor is there any national circular concerning ML, despite the work done on this by the Ecofin Network of the public prosecutor's offices since 2009.⁵ In particular, there is no strategy or co-ordination between the different public prosecutor's offices and investigating judges responsible for ML investigations. Practices differ from one district to the next, and even between different judges, signifying a lack of methodology. Finally, it is impossible to make an overall assessment of whether ML activities are actually investigated and prosecuted commensurate with the level of risk.

3.54. According to the Brussels public prosecutor's office, **the main criteria for initiating** proceedings are all of the following: the current or future possibility of seizing sums of money, the seriousness of the

3 See FATF (2005), para. 51, 292, 467.

4 In an attempt to make the judicial system more rational, the number of judicial districts was cut from 27 to 12 (Law of 1 December 2013). The Public Prosecutor's Offices serving them also receive ML cases.

5 The work that this network of experts on combating economic and financial crime does with the law enforcement authorities on ML is limited and does not make up for a lack of guidance (the organisation was set up by legislation and has been operating officially since 2003 and informally since 1997).

3

predicate offence (terrorist financing, trafficking of property or drugs, fraud, serious and organised tax fraud, people trafficking, organised crime, exploitation of prostitution), the ability to investigate and prosecute (the Public Prosecutor and the police must have sufficient resources to see the case through) and the existence of a significant amount of laundered money. **These criteria do not take any account of the sectors identified as having a high risk of ML** or the difficulties of ML investigations. The criteria have been mainly due to the workload and lack of staff with the public prosecutor’s office, particularly in the francophone section of the Brussels public prosecutor’s office.

3.55. **The number of cases related to precious metals or diamonds is limited**, which is surprising given the size of these markets in Belgium and the risks they pose: The Belgian authorities cited around ten sentences related to the diamond sector since 2003 (certain of these were linked to human being and narcotics trafficking; others with tax fraud); one case led to a plea bargain of EUR 10 million with tax fraud as the predicate offence . The Belgian authorities also mentioned two significant cases that are in progress (one of these for ten years), involving suspected organised ML. The observation is the same both for cross-border transportation of cash, for which the number of proceedings does not appear to be commensurate with the number of indictments made, and for legal persons and legal and/or financial professions, for which the activities and risk are considered to be significant, according to a study by the Federal Police (see *Security 2011: the Police View* incorporated into the development of the National Security Plan 2012-2015).

3.56. The deficiencies identified in the national risk assessments, including the lack of any method for determining the biggest threats and the most vulnerable sectors, coupled with the lack of statistics for investigations, make it difficult to determine whether the level of investigation of ML activities is commensurate with the level of risk.

3.57. Despite having limited criteria for launching investigations and proceedings, the public prosecutor’s offices still initiate a **large number of proceedings for ML**, either alone or in conjunction with predicate offences. **For 2013, the total number of registered ML cases was 1 762 for all the public prosecutor’s offices in Belgium** (2 105 in 2012, 1 866 in 2011) (this represents 0.24% of new cases on average and 0.6% of cases sent for judicial investigation). For the years 2005-2013, the public prosecutor’s office estimated that about half of the cases had received or were to receive ‘criminal follow-up’⁶ (and half were to be closed). Therefore, it is estimated that the number of judicial investigations (*informations et instructions*) opened each year relating to ML amounted to a little less than 800 for this period. This is evidence of significant activity in the area of criminal ML investigations.

Table 3.4. Number of ML Cases Received by Public Prosecutor’s Offices from 2005 to 2012

2005	2006	2007	2008	2009	2010	2011	2012
1 128	1 311	1 716	1 409	1 376	1 658	1 865	2 108

Source: Database of the College of Prosecutors General – statistical analysts.

6 The Belgian public prosecutor’ office indicated that the possible legal outcomes in criminal cases include the following : plea bargain ; mediation ; summons, hearing and decision (after an investigation by the prosecution authority [*information*]; judicial or in chambers investigation(*instruction ou en chambre du conseil*); hearing and decision (after judicial investigation); closure with no further action but with a court supervised probation; or administrative fine. This does not take into account the decisions made by investigative and tribunals; cases where the proceedings were closed without trial or resulted in acquittal of the defendant are also possible legal outcomes in these cases.

(b) Success of investigations and prosecutions

3.58. Among their successes, the Belgian authorities mentioned the following ML cases:

Box 3.1. Successful money laundering cases**Co-operation between FIUs**

The Belgian public prosecutor's office launched an investigation based on information received from CTIF, which was based on a report received from a foreign FIU (Guernsey). A sum of USD 10 million from an account in the name of a company in Dubai had been deposited in an account opened at a local bank by a company registered in the British Virgin Islands. One of the beneficial owners lived in Brussels and had already been convicted in Belgium of a very large VAT fraud.

The investigation by the public prosecutor's office could not establish the legal origin of the USD 10 million transferred to Guernsey. The good relationship between the Belgian investigators and the authorities in Guernsey prompted a quick reaction leading to the freezing of the funds pending letters rogatory and referral to the Belgian authorities. This referral will make the funds subject to confiscation orders issued by the Belgian courts and should enable the suspect's unpaid tax debts to be partially liquidated.

Money laundering without a predicate offence

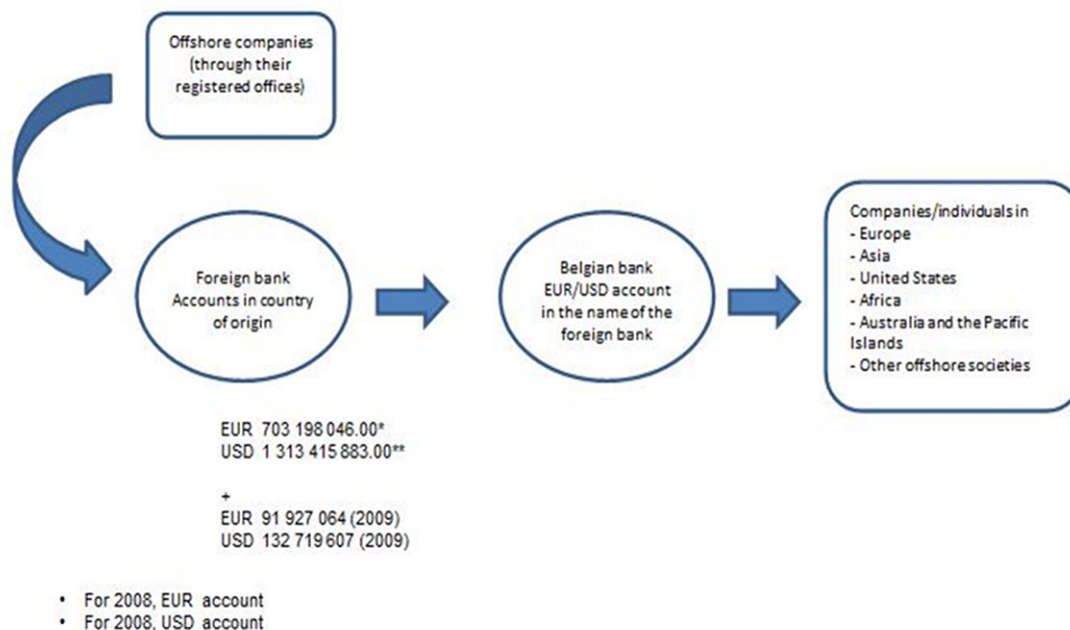
An appeal court confirmed the conviction for ML of a person even though the origin of the funds had not been ascertained. The judges considered that any lawful provenance for the funds used to buy the assets concerned could be ruled out. The funds in this case (nearly EUR 5 million), of unknown origin, were invested in companies and property in Romania and Canada. The judges observed that the funds subject to ML could not have come from the official personal incomes of the appellants, nor profits from their company, donations or inheritances, and nor could they have come from the activities that the appellants claimed they were from.

3.59. These cases illustrate the Belgian authorities' ability to handle ML cases by means of detailed investigations. However, an examination of some other cases presented by the Public Prosecutor (23) shows that most ML investigations relate to ML offences committed in Belgium in association with predicate offences also committed in Belgium. **Most prosecutions for ML are for self-laundering.** The patterns that appear most frequently are cases of fraud, tax fraud and drug trafficking in Belgium where the proceeds are laundered in Belgium. Where legal persons are involved, they are actually instrumentalities created by natural persons, and where they are prosecuted they tend to end up being acquitted (in the examples supplied).

3.60. The Belgian authorities reported a few cases where organised ML schemes, and third parties were involved in the predicate offences. In the first case, two payable-through accounts were opened in Belgium in the context of correspondent banking activities by a bank established in an Eastern European country, for the purpose of paying through funds belonging to multiple offshore companies (customers of the bank) to various counterparties all over the world. The case was closed without being followed up because court proceedings had already been initiated in the country where the bank was established, and the evidence had therefore been sent officially to the authorities in the other country in application of the EU Convention on Mutual Assistance in Criminal Matters.

3.61. Two other cases involving organised ML schemes and 3rd party ML with predicate offences linked to the diamond trade sector are in progress (one for a number of years); however, these were not discussed (see below on technical problems).

Chart 3.1. Money laundering through offshore companies



3.62. **The law enforcement authorities each have their own databases** (public prosecutor's office, investigating judges, courts) **but they are not linked together.** Only the Federal Prosecutor's Office was able to provide statistics, though these were prepared using manual counting methods because of the small number of cases it handles. The database shared by all the public prosecutor's offices is out-of-date and was designed not for statistical purposes but for administrative ones, and therefore cannot provide a break down by crime. It indicates the stage in proceedings of a case and what the main charge was when the case was first entered in the system, but this information is of no use for a qualitative analysis. This problem had already been identified in the 2005 MER (paragraph 49). CTIF also has for its part, statistical data on criminal proceedings, including on the number of convictions of persons charged and confiscations, as far as the cases are based on CTIF reports. Nevertheless, the statistics do not distinguish between ML cases and those involving other offences. They use different criteria and were created for different purposes. Based on this observation, the statistical data of the prosecution authorities and the CTIF cannot be compared or used appropriately.

3.63. **There are a number of factors that lessen the chances of success of ML investigations and prosecutions in Belgium.** As indicated in IO 6, the data supplied do not reveal the existence, still less the number, of **parallel financial investigations** for the purpose of sanctioning potential criminals effectively. Nor is it possible to find out how many cross-border ML investigations are conducted or investigative measures are taken by the Belgian authorities in this context (reports of predicate offences committed in Belgium with ML abroad and vice versa), though examples of this do exist⁷ and the public prosecutors and investigating judges met by the assessors say that they often make use of mutual assistance. This is an important matter given the identified risks of cross-border cases.

3.64. ML cases, particularly cases where the assets are of high value, and cross-border cases, are not a clearly defined priority.

⁷ *Cassation*, 20 November 2013, concerning a conviction in Belgium for laundering the proceeds of an offence committed abroad (but subsequently closed); and conversely Antwerp Court of Appeal, 19 December 2013, for the laundering in Belgium of the proceeds of offences committed abroad by a Belgian resident.

3.65. The consequence of this is that the number of cases closed without being followed up, for expediency or criminal policy reasons (insufficient means of investigation, other priorities), is high and is increasing.⁸

- 2010: 46.4%, of which 14.5% because of insufficient investigative means and 31.9% because of other priorities;
- 2011: 42.9%, of which 14.6% because of insufficient investigative means and 28.3% because of other priorities;
- 2012: 55.9%, of which 17% because of insufficient investigative means and 38.9% because of other priorities.

3.66. This finding reveals that **the Belgian law enforcement authorities have insufficient resources** for investigating ML. Moreover, it is not possible to find out what proportion of cases are closed without follow-up once the judicial investigation has begun. The number of ML cases where the case is dismissed is not known either.

3.67. **The statistics provided by Belgium for convictions** for ML show not the number of people convicted but the number of offences judged to have been established, with the consequence that the same person is often convicted for several ML offences (Art. 505(1)(2), (3) and/or (4)). If a person has committed three types of ML offence, the statistics count three occurrences. The figures do not show the number of people convicted because it is common for a person to have committed multiple ML offences and the number of convictions per offence is much higher than the number of people convicted.

Table 3.5. Number of convictions for each type of ML offence

	2006	2007	2008	2009	2010	2011	2012	2013 (nov.)
505(1)(2) illegal transactions using the proceeds of offences	157	197	141	102	115	154	138	70
505(1)(3) conversion or transfer	87	99	95	130	92	97	82	33
505(1)(4) concealment of origin	51	61	50	52	28	41	48	20

Source: FPS Justice - Criminal Policy Department

3.68. These figures, though high for the size of the country, should be examined in conjunction with the information received about quality: once again, **a large number of these convictions are secured in domestic cases for self-laundering**. Convictions of third parties for ML appear to be rare. Comparing the data for the number of investigations launched by the public prosecutor’s office and the number of convictions is impossible and the success rate can therefore not be determined. According to a CTIF study relating to the period 2005 to June 2014, for the cases sent by CTIF to the public prosecutor’s office and for which a sentence had been handed down, the following observation can be made: 550 persons out of 2 332 persons involved were not prosecuted or convicted for ML. In these CTIF cases, 1 483 persons received a prison term, 1 240 received a fine and 589 were subject to confiscation (whether for ML or not). Moreover, for all verdicts: 51 cases were considered to be beyond the statute of limitations; 50 cases resulted in sentences of community service; 153 cases were acquittals; for 70 cases the sentence was deferred; 37 cases were simple guilty verdicts; 15 cases were declared inadmissible; for 1 case the court was determined not to have territorial jurisdiction. This observation illustrates the difficulty encountered by Belgian authorities in the effectiveness of their criminal prosecutions.

8 CTIF likewise indicated that in the last 10 years, 62% of cases sent to the public prosecutor’s offices have been closed without being followed up.

3

3.69. On the other hand, Belgium has a number of recorded cases of **ML convictions without a conviction for the predicate offence**, as shown by a CTIF study of the court judgments it was able to gather (see table below). This is possible chiefly because of Art.43 *quater* PC, which also provides for confiscation with division of the burden of proof between the public prosecutor’s office and the accused as regards the origin of the assets to be confiscated (see IO 8).

Table 3.6. Sample of 599 convictions between 2007 and 2014 stemming from CTIF reports forwarded to the Public Prosecutor’s Office, of which CTIF received a copy

Convictions for ML only	167 offences
Convictions for ML linked to one or more crimes covered by AML/CFT Law	432 predicate offences
ML not accepted by the public prosecutor’s office	157 verdicts
ML not accepted by the court	53 verdicts

Source: CTIF

3.70. The law enforcement authorities have identified certain technical difficulties:

- **Convictions of legal persons are difficult to secure** (Art. 5 PC), because the legislative framework is complex to apply (many criteria have to be met). The Belgian authorities explain that this is due to a number of factors: legal persons are often merely ‘fronts’ without any actual financial existence; legal persons have ceased to exist by the time the criminal case is brought; legal persons tend more to be victims of ML operations. Criminal prosecution authorities tend to focus more on the natural persons that set up the legal entities in order to launder money. However, the Federal Judicial Police are running a project to detect suspicious capital increases as part of ML schemes. In one example judgment provided, the legal person used to launder some of the misappropriated funds, was prosecuted for ML but was acquitted because the court decided it had no independent volition apart from the main defendant (who was convicted for producing fraudulent invoices; Brussels Court of Appeal, 10 October 2013). However, some cases of structured ML involving legal persons have been detected. In two other cases, some financial institutions entered into plea bargaining with the Public Prosecutor in 2013 and 2014 in cases of the laundering of tax fraud committed by customers, respectively for EUR 2.2 million and EUR 700 000. Legal persons account for less than 2.85% of all persons involved in ML cases opened by the public prosecutor’s office (for the period 2005 to 2012).⁹

- **Plea bargaining (simple or extended)**: because the plea bargaining measure was inappropriate in the case of complex economic and financial crimes, particularly concerning ML, the scope of the procedure was amended in 2011 to include ‘**extended plea bargaining**’ (Art. 216 *bis* CCP). This measure is the response of the public prosecutor’s office to the risk of exceeding the statute of limitations or a ‘reasonable time’ for the proceedings.

Example: In a case opened in 1996, principally for acts of ML dating back to 1992, an extended plea bargain was agreed in 2011 by the *Prosecutor General*, Brussels Court of Appeal, for the sum of EUR 22 million (in this agreement there was also the confiscation of property linked to these offences.)

- Extended plea bargaining was offered in 67 ML cases (mainly in Antwerp) and ordinary plea bargaining in 117 cases (the number of plea bargains concluded is unknown). Since August 2011, 17 extended plea bargains were agreed for cases of the local public prosecutors that had either

⁹ Source: Database of the College of Prosecutors General – statistical analysts.

ML as the sole offence or as accessory offence. The results are not consistent: while the financial benefits abandoned by persons seems to be above the amount of the suspected ML, certain amounts linked to plea bargains are less than 5% of the amount of suspected ML. Plea bargaining allows for proceedings to end with the agreement of all parties: amounts up to EUR 23 million have been collected; agreements deal with payment tax fines. The Federal Prosecutor's Office never cites ML prevention as justification for executing seizures abroad because certain countries require proof of the predicate offence. For this reason, there is no plea bargaining involving ML prevention for the Federal Prosecutor's Office. Although this measure has the advantage of ending up with the application of a fine and/or confiscation in cases that could otherwise have been struck off under the statute of limitations or might have failed due to a lack of investigative resources, **it leaves no trace on a person's criminal record** and can therefore pose problems, particularly in the event of repeat offenders (as well as concerning 'fit and proper' accreditation and checks carried out management and shareholders (see Section 6.3(a)).

- **The application of Belgian legislation** (the 'Franchimont' Law¹⁰) revealed the use of rights granted to the defendant **purely as delaying tactics** in ML cases. The use of certain rights tends to push the proceedings beyond the statute of limitations in criminal cases. The parties may, at any time after the investigation stage is finished, ask for certain additional procedural formalities to be completed, the execution of which can delay the proceedings by several months, and they can do this more than once. To remedy this, the Belgian parliament has moved to allow the statute of limitations to be suspended under certain conditions.¹¹

3.71. CTIF has for some years been drawing politicians' attention in its annual reports (1996, 1999, 2000 and current) to the fact that the judicial follow-up of ML cases forwarded by CTIF to the judicial authorities is 'a problem that has been raised on numerous occasions and deserves particular attention'.¹²

3.72. These difficulties have an impact on the handing down of sentences. **It is impossible to say whether the sanctions applied are effective, proportionate and dissuasive** because most persons are convicted for several offences, including ML. Thus, the sanctions handed down sometimes exceed the legal minimum foreseen for ML (five years) as a result of the aggregation of offences. Conversely, certain persons are sentenced to lower fines (EUR 200-2 000) without imprisonment. On the basis of the verdicts for CTIF cases, it can be observed that the sentences of imprisonment (handed down for ML alone or along with other offences) are most often under one year (45%), and 62% are under two years. When deciding the severity of the sanction, the courts take into account the previous criminal record of the convicted person, the degree of involvement in the offence and the reasonableness of the proceedings (the dissuasiveness of the sanction). For further information on this, see the table below, which is based on the CTIF cases that have resulted in a verdict, whether for ML or other offences.

10 Law of 12 March 1998 on the improvement of criminal procedure at the police investigation and judicial investigation stages (police investigation is led by the public prosecutor's office, and judicial investigation by the investigating judge).

11 Law of 14 January 2013, which entered into force on 10 February 2013.

12 See also CTIF, *White Paper on Black Money*. CTIF (2013), page 35.

Table 3.7. Prison Terms Handed Down for CTIF Cases (ML or Other Offences)

Number of persons convicted	2005	2006	2007	2008	2009	2010	2011	2012	2013	Total	%
≤1 year	158	95	86	63	70	49	82	40	23	666	45.15 %
1 - 2 years	67	51	38	49	49	31	33	20	17	355	24.06 %
2 - 3 years	53	17	36	36	21	24	12	13	6	218	14.8 %
3 - 4 years	28	9	16	14	12	15	10	3	8	115	7.80 %
4 - 5 years	9	2	14	9	22	9	2	4	6	77	5.20 %
≥ 5 years	19	0	3	6	2	9	2	2	1	44	2.99 %
Total	334	174	193	177	176	137	141	82	61	1 475	100 %

Source : CTIF

3.73. The court takes into account offences committed, the criminal record of the person and the reasonableness of the length of the proceedings, etc. On the basis of data provided by the Belgian authorities, it was not possible to determine with any accuracy the amount of fines incurred for ML cases. Finally, the 1999 law provided for the recording of convictions of legal persons in a legal persons' criminal record held at the court registry, but this system is not yet in place (see Section 7).

3.74. **The public prosecutor's office has stated that some of these deficiencies are due to a lack of human, material and documentary resources;** however, it tries to do its best with the limited resources allocated to criminal law authorities: Not all cases are entered into the computer system yet, resulting in a failure to follow them up and an increased risk of the case files or parts of them going astray or being misfiled. The fact that judgments are not classified and stored electronically also means that knowledge of them is lost and makes it more difficult to analyse the jurisprudence. The judges from the public prosecutor's office do not have full electronic versions of case files at hearings, which can cause difficulty in very big cases. The public prosecutor's office and the investigating judges are not given any special training on ML; however, many of them have a basic knowledge of accounting and expertise in economics. The public prosecutor's office is considering organising special training on ML and setting up a platform for sharing experiences.

3.75. Several important case files that CTIF had sent to the judicial authorities concerning the laundering of significant sums of money were not followed up because **the acts were beyond the statute of limitations or a 'reasonable time' for the proceedings had been exceeded.** Some court judgments revealed cases of exceeding the statute of limitations and sentences shortened due to the length of the proceedings.¹³ For the same reasons, a certain number of convicted persons received no sentence despite the guilty verdict handed down by the court. Such proceedings, which appear to be quite common according to those that the assessors met in Belgium, prevent effective and dissuasive sanctions from being handed down. This also has implications for confiscations since they are linked to convictions; this was also commented on by one of the sitting judges met by the assessors. The shortage of personnel at the public prosecutor's offices and courts of appeal does affect timescales, but certain technical issues (explained above) are also to blame. The OECD already indicated in 2005 – and noted with greater emphasis in 2013 – the lack of resources of the prosecution authorities and its effect on criminal proceedings in the area of transnational corruption.¹⁴

13 See in particular Judgment of the Brussels Court of Appeal, 21/10/2013 (not final because of an appeal to the *Cour de Cassation*), Judgment of the Brussels Court of first instance, 26/06/2012, Judgment of the Brussels Court of first instance, 15/05/2012 and Judgment of the Brussels Court of Appeal, 07/05/2013.

14 OECD: *Reports on Implementing the OECD Anti-Bribery Convention in Belgium* ; Phase 2 in July 2005, Phase 3 in October 2013.

3.76. **In conclusion, the Belgian authorities are imbued with the culture of combatting ML.** They also have the necessary investigative techniques. In consequence, there have been a significant number of convictions for ML in Belgium. Moreover, it is not unusual for convictions to be obtained without the predicate offence being proven due to the distribution of the burden of proof in certain cases of ML. **However,** prosecutions are most often focussed on the predicate offences where ML is an additional charge against the same person (self-laundering).

3.77. **The number of cases highlighting structured ML schemes where third parties assist with laundering of the proceeds from offences committed by the main offender are limited.** For some offences, particularly those involving the cross-border transportation of cash, precious metals and diamonds, the number of prosecutions is not commensurate with the level of risk cited by the Belgian authorities.

3.78. **The scope of actions to combat ML is limited** by the absence at the national level of an overall AML strategy and co-ordination among prosecutors responsible for ML cases. **A lack of resources,** material means, training and co-ordination among the law enforcement authorities reduces their effectiveness. **Too many cases are closed for reasons of expediency,** reducing the criminal justice response rate. In addition, the length of certain criminal proceedings results in the statute of limitations being exceeded or reduced severity of the sanctions.

3.79. However, in the context of the evaluation and its preparation, the Belgian authorities revealed the existence of deficiencies and expressed a desire to raising the priority of ML prosecutions, and gave examples to support this.

3.80. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 7.**

3.5 Effectiveness: Immediate Outcome 8 (Confiscation)

(a) Priorities

3.81. The Belgian authorities see confiscation of the proceeds and instrumentalities of a crime, or property of a corresponding value, as being one of the main objectives of AML activity. So training in seizure and confiscation is mandatory for future judges. During these sessions, the OCSC passes on best practices and actions to be avoided, emphasising the need to make confiscations more effective. The legislative framework, which is sophisticated and comprehensive, allows the seizure and confiscation on a large scale of all assets that have been laundered or are the proceeds of predicate offences (see R 4). The system in place also allows the confiscation of assets of a corresponding value where the direct proceeds of offences are no longer available. However, it should be remembered that confiscation is an additional penalty (*peine accessoire*) tied to a criminal conviction.

3.82. The **Brussels public prosecutor's office**, which specialises in AML, **uses the possibility of seizing assets with a view to their confiscation as a criterion for prioritising cases**, because of the large number of cases to be processed. Investigating judges also recognise the importance of this criterion. However, the statistics presented are fragmented (see below). The police have been made aware of the need to direct their investigations towards the proceeds of crime: an indicator was introduced in 2013 to monitor the amounts seized, as part of a programme to recover illegally gained and laundered assets,¹⁵ but its impact has not yet been evaluated.

3.83. **The prosecution authorities have the power to order detailed financial investigations** to detect any assets to be seized and subsequently confiscated, and not only those that are directly available (see IO 6). These investigations can cover assets held abroad as well as those held in Belgium. They can be linked both to

15 The police set up this programme in 2012 following the publication of the 2012-2015 National Security Plan, approved by the Justice and Interior Ministers, in application of Art. 95 of the integrated policing law.

3

the predicate offence and to ML. Information provided makes it difficult to determine whether the authorities use these measures systematically, regularly or just occasionally. Investigations aimed at obtaining the confiscation of additional assets may also be carried out where it can be presumed, on the basis of serious material indicators, that the assets were generated by ML or TF (this measure is available only for a few offences; Art.43 *quater* PC, see the 2005 MER, paragraph 155). An investigation of this kind may be requested by the public prosecutor’s office or ordered by the judge who handed down the guilty verdict (Art. 524 *bis* CCP). The Belgian authorities were unable to provide statistics or examples of the use of this measure in ML cases.

3.84. Belgium strengthened its capacity to trace assets by passing, on 11 February 2014, the Law on various measures aimed at improving the **recovery of assets** and costs in criminal cases (I and II) (entry into force on 18 April 2014, inserting Art. 464/1 to 464/41 CCP). This law improves the effectiveness of confiscation ordered by the courts by creating an enforcement investigation in criminal cases (*enquête criminelle d’exécution*), defined as a set of actions aimed at identifying, tracing and seizing assets where a conviction requiring payment of a fine, a special confiscation, or payment of legal fees is to be enforced. Proceedings are organised at the direction of a specialist judge from the public prosecutor’s office, by the OCSC, or with its support. The competent authority has extensive means of investigation for tracing assets so that asset-related sentences, particularly confiscation, can be enforced. Because the law is so recent, it is not possible to say at this stage how effective it is, but it shows the priority given by the Belgian authorities to depriving criminals of the proceeds of the offences they commit.

3.85. As far as provisional measures are concerned, **CTIF has the power to block financial transactions** (for up to five days) when a report has to be sent to the to the public prosecutor’s office and there is a danger that it will no longer be possible to seize funds.

Table 3.8. Measures to block financial transactions

	2009	2010	2011	2012	2013	Total
Number of blocking measures	38	60	33	36	25	192
Amount (EUR millions)	10.47	135.84	183.59	11.81	12.34	354.05

Source: CTIF

(b) Central Office for Seizure and Confiscation (OCSC)

3.86. **The OCSC, a specialist unit** attached to the public prosecutor’s office, has been operational since September 2003. This unit, which has around 37 staff, some of whom are liaison officers from the police and the tax authorities, is responsible for **maintaining the value of seized property and enforcing court confiscation orders**. In practice, the OCSC has observed a marked preference among judges for the rapid disposal (sale) of seized property that depreciates rapidly (goods, vehicles, buildings, etc.), enabling these to be replaced by a sum of money. In this task the OCSC works closely with FPS Finance.

Table 3.9. Amounts seized in OCSC cases (EUR)

	2011	2012
Organised crime	2 547 116	1 418 510
Misappropriation/embezzlement	3 732 420	6 387 482
Money laundering	91 192 415	23 127 457
Drugs	5 561 511	9 162 763
Tax fraud	5 014 613	3 287 444

Source: OCSC, Evaluation of the threat, risks and vulnerabilities in relation to ML, 16.12.2013; p. 149. Numbers for 2013 were not available.

Table 3.10. Number of sales of seized property (to avoid depreciation) all types of offences

Year	2006	2007	2008	2009	2010	2011	2012	2013
Number	327	259	541	947	1 691	1 481	2 230	2 059

Source: OCSC

Table 3.11. Number of confiscations of property of a corresponding value by the OCSC (all types of offence)

Year	2006	2007	2008	2009	2010	2011	2012	2013
Number	1 051	1 114	1 375	1 705	1 741	1 856	1 447	1 448

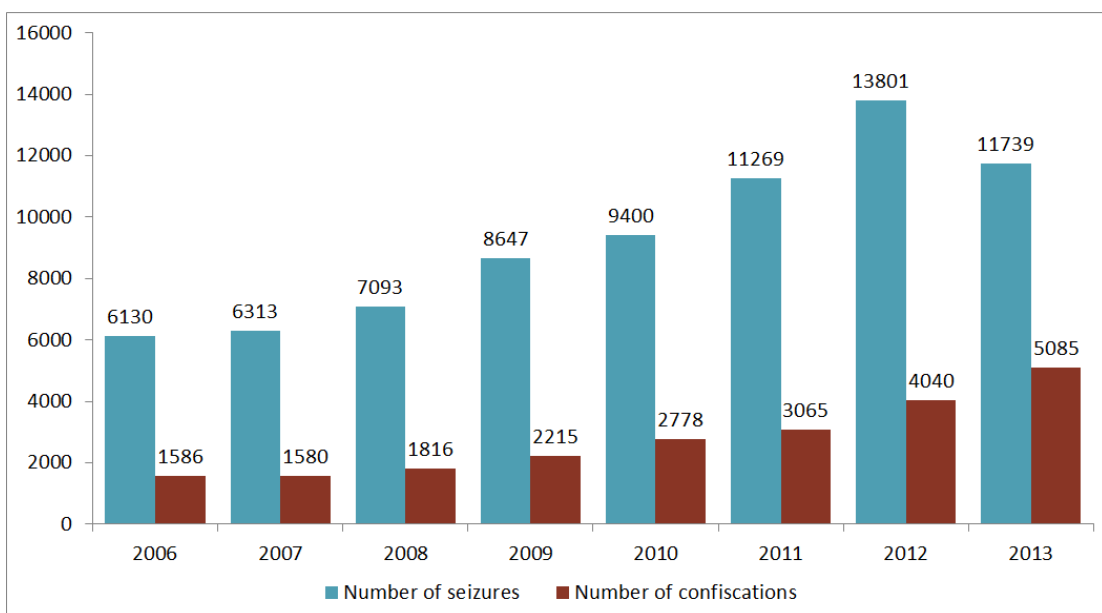
Source: OCSC

Note: During proceedings to enforce the confiscation of assets of a corresponding value, the OCSC sends a mandate to the relevant revenue collector (FPS Finance) to contact the convicted person and recover the sum determined by the trial judge. The OCSC only has statistics for the number of confiscations of assets of a corresponding value ordered by trial judges and not for the amounts actually recovered by the revenue collectors.

3.87. The OCSC also provides advice and training for the judges concerned in order to improve the confiscation process and the effectiveness of the proceedings, particularly proceedings for the **confiscation of assets of a corresponding value**.

3.88. **The OCSC’s resources and means are appropriate for its current responsibilities.** In practice, the OCSC is not automatically involved in all seizure and confiscation proceedings. Although the police regularly refer seizure cases to the OCSC, the same cannot be said for judges (public prosecutors, investigating judges and trial judges). The OCSC is not informed about many seizure and confiscation proceedings, either as regards the values involved or the grounds (offences), despite the fact that one of the OCSC’s responsibilities is to **collect, manage and process all the data** concerning seizures of property and its conservation or storage, and confiscations and the judgments to which they relate (in a database). However, its involvement is increasing over time, as shown by Chart 3.2.

Chart 3.2. Number of seizures and confiscations registered by OCSC



Source: OCSC – by number of cases

3

3.89. Based on the information gathered during the evaluation visit, the conclusion can be drawn that the OCSC’s role consists mainly of placing the seized sums (currently around EUR 500 million) in a bank account and disposing of assets where their maintenance or management could be problematic (e.g. buildings occupied by tenants) or they could rapidly depreciate (e.g. vehicles). In addition, the OCSC makes various low-risk, liquid financial investments to maintain the value of seized assets. The OCSC’s resources will therefore have to be increased in line with its growing role in the management of seized property and its involvement in the implementation of the 2014 law on the collection of assets for confiscation.

(c) Effectiveness of seizures and confiscations in practice

3.90. **Full use is made of the legislative framework, which is sophisticated and comprehensive** – all the available measures have been used by the Belgian authorities in ML cases. Case examples were provided to demonstrate this, for example concerning the confiscation of real estate located abroad (*Cassation*, 17 December 2013), the sale of perishable seized goods, the confiscation of assets of a corresponding value from a third party, with restitution to the victims (Brussels Court of Appeal, 10 October 2013); the confiscation from third parties of property acquired together with the proceeds of the offence (*Cassation*, 4 March 2014); the confiscation of assets of a corresponding value of a portion financed by the proceeds of the offence of a property bought jointly with a *bona fide* third party (Liège Court of Appeal, 20 May 2009).

3.91. However, the experiences and examples recounted by the Belgian authorities **do not demonstrate in any significant or convincing way the effectiveness** of confiscation proceedings, particularly in cases of **cross-border crime** or activities that represent **ML risks and vulnerabilities** for Belgium.

3.92. Moreover, the information, statistics and data presented by the Belgian authorities as regards seizure and confiscation make it difficult to evaluate satisfactorily the effectiveness of the confiscation measures and whether they reflect the evaluated ML risks:

- An internal study by CTIF of the court decisions handed down in cases related to its reports found that the confiscations ordered for the period 2005 to 2014 totalled EUR 600 million.

Table 3.12. Confiscations 2005 - 2014

Year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Amount (millions)	111.95	41.45	43.93	51.89	34.01	67.19	41.96	149.91	44.93	12.52

- The confiscations included were not only ML (when such a conviction was cited) but also all (predicate) offences prosecuted. The majority of the significant confiscations ordered were related to tax fraud and narcotics trafficking.
- The statistics and data supplied for seizure and confiscation are not presented in a consolidated format, making it difficult to interpret how well they meet the effectiveness criteria. The information provided is incomplete and not sufficiently precise, and therefore unreliable, on two levels. On the one hand, the figures supplied do not give a realistic or meaningful picture of the situation because they are based mainly on the OCSC database, which only records cases where there is OCSC involvement (see above). On the other, the information provided only rarely mentions the offences in which the seizures and confiscations originated.¹⁶
- The statistics do not provide enough qualitative information to judge the effectiveness of seizures and confiscations and asset sharing with other countries, or the restitution of confiscated funds to victims, even though several actual cases of asset sharing were presented (see Section 8) along with case examples showing the restitution of funds to victims (e.g. Brussels Court of Appeal,

16 This observation has already been made by the OECD. See OECD (2013), especially page 5.

10 October 2013). The OCSC indicates that, as regards asset recovery, a new database is currently being set up with assistance from the Federal Police.

3.93. **In practice the OCSC plays only a limited role in managing assets** because it is not systematically consulted or informed by the authorities, though its involvement is increasing over time, as explained above. The OCSC, which intends to become a centre of expertise in seizure and confiscation and to play a technical assistance role, has **only a partial picture of seizures** and confiscations and their outcomes, considerably weakening its role and competencies. In principle, the OCSC should be notified of every seizure of EUR 2 500 or more. However, the authorities say that there are sometimes delays in recording these seizures (by the police or investigating judges, for example), which means that the OCSC database is not up-to-date. The figures submitted are therefore minimum figures because they do not take account of seizures and confiscations made without the OCSC’s assistance. Furthermore, few judges seek assistance from the OCSC, though the OCSC has seen an increase in this too, with cases where judges have sought practical help (e.g. Brussels Court of Appeal, 10 October 2013, a case in which the OCSC sold most of the seized property for a total of EUR 2.8 million).

3.94. Until February 2014 the OCSC’s work consisted of asset management. Since the Law of 11 February 2014 was passed, **particular emphasis has been placed on the recovery of assets** with the particular aim of stepping up the search for assets that could be confiscated. As explained earlier, this is a recent law and it is therefore not possible to assess its effectiveness at this stage. Although a circular in May 2014 aimed to raise awareness of this new law among public prosecutor’s offices, the implementing text is currently in preparation.

3.95. Under Belgian law, confiscation is an additional penalty (*peine accessoire*) in that it remains linked to a criminal conviction. Consequently, confiscation cannot be envisaged if the defendant is not convicted. Based on the statistics and explanations provided by the Belgian authorities, there are many proceedings for ML that do not end up in a conviction for criminal policy reasons, because of the length of the proceedings (dispersal or deterioration of the evidence) or because the statute of limitations has been exceeded. This means that **a large number of potential confiscations cannot be completed. The deficiencies in the criminal justice response (see IO 7) therefore have direct and important consequences as regards confiscation.**

3.96. **The OCSC is a member of the CARIN network** and is the recognised Asset Recovery Office for Belgium in the EU.¹⁷ The OCSC has submitted and fulfilled mutual assistance requests, with a marked increase in outgoing requests both inside and outside the EU (see Table 3.13).

3.97. The increase in these figures may be explained by the gradual transposition of European laws into the national legislation of the Member States, facilitating co-operation between them. Notably, the number of outgoing requests is higher than the number of incoming requests, both generally and specifically for ML (except in 2013).

Table 3.13. Mutual assistance requests (OCSC) for all types of offences

Year	2010	2011	2012	2013
Requests made to foreign authorities	113	164	221	224
- Of these, for money laundering	39	59	48	24
Requests received from foreign authorities	63	72	67	124
- Of these, for money laundering	16	7	12	33

Source: OCSC

17 Established in 2004, the CARIN network (Camden Assets Recovery Inter-Agency Network) based at the Europol headquarters is an informal network of legal practitioners and detection and enforcement services specialising in tracing, freezing, seizing and confiscating the proceeds of crime.



3.98. Once again, mutual legal assistance is not only requested via the OCSC for seizures and confiscations. In the case mentioned above (Brussels Court of Appeal, 2013), the prosecution authorities asked for a bank account held abroad to be identified and frozen.

3.99. The Belgian authorities say that mutual legal assistance requests made with a view to confiscation abroad are not always carried out, particularly when the conviction in Belgium is for ML but there is no conviction for a predicate offence.

3

Cross-border currency movements

3.100. In the context of cross-border movements of currency or bearer negotiable instruments, where a false declaration/no declaration is made, or a false disclosure is made, cash seizures are made every year by AGDA and the national judicial police. In 2013, these services were once again reminded of the importance of checks, particularly as regards sums of money leaving Belgium related to the risk of drug trafficking, and of several best practices. AGDA has taken steps to control cross-border cash movements, particularly by making targeted checks. Since February 2014, a team specialising in this type of check has been operating at Zaventem international airport. Systematic checks are also made on some trains.

3.101. The money seized (around EUR 157 000 in 2011; around EUR 1 million in 2012) is available to the public prosecutor's office, but there are no data from which the number of confiscations of cash made outside the *Cash Watch* programme can be determined. There were 49 cases within the programme in the 2009-2013 period, amounting to a total of EUR 7.6 million. These cases resulted in 18 convictions, seven plea bargains and four case closures. The other 20 cases are not yet finished. This number of cases seems low compared with the period. Other examples of convictions for ML have been provided, often without the predicate offence being determined (ML as a stand-alone offence), where the currency being transported was confiscated.

3.102. Representatives of the public prosecutor's office indicated that, because of workload and many cases being behind schedule, the 14-day administrative seizure is rarely extended by a judicial seizure, but particular attention seems to be paid to *Cash Watch* operations.

3.103. The Belgian customs service (AGDA) makes practical use international co-operation, co-operating particularly with the French customs service. The majority of sums seized in 2012 were seized as a result of this co-operation.

3.104. ***In conclusion***, the information provided by the Belgian authorities shows that there are seizures, confiscations, and confiscations of assets of a corresponding value in ML cases. However, although the authorities are keen to prioritise prosecutions that lead to confiscation, they are not always entirely successful in this. The prosecution authorities have indicated that emphasis is placed on confiscation, but the information provided does not reveal evidence of any such objectives having been set or any systematic search during financial investigations for assets that could be confiscated. However, confiscations are regularly made of readily available and easily identifiable proceeds of offences. Lack of effectiveness as regards criminal prosecutions (length of proceedings, lapsing of the statute of limitations, etc.) also has an impact on confiscations.

3.105. **The Belgian authorities do not have any relevant or clear centrally-held statistics** for seizures and confiscations of assets in Belgium or abroad, asset sharing, the offences in which the seizures or confiscations originated (ML and the predicate offences), confiscations related to false disclosures or declarations at borders, or the amounts returned to victims. It is therefore difficult to evaluate the tracing undertaken and results achieved in these areas.

3.106. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 8.**

3.6 Recommendations on legal system and operational issues

Financial Intelligence (Immediate Outcome 6)

- The law enforcement authorities should step up the search for financial intelligence and the processing of this intelligence, particularly on the basis of the case files and other information supplied by CTIF.
- Those involved in AML/CFT activity, particularly the law enforcement authorities, should improve co-ordination and the exchange of information with one another (forwarding, processing and feedback). Establishing a unified approach and reinforcing relationships within prosecution authorities should help with this.
- Appropriate statistics and databases should be introduced so that the research and exploitation of information useful and necessary for criminal proceedings can be defined and their effectiveness evaluated.

ML investigations and prosecutions (Immediate Outcome 7)

- Belgium should define a clear criminal justice policy that identifies the prosecution of ML as a priority, and should define the resources necessary for prosecuting and punishing ML commensurate with the main risks identified.
- The prosecution authorities should have appropriate (human and material) resources and technical means (IT, databases) at their disposal for the effective criminal prosecution of ML.
- Judges responsible for ML prosecutions should receive more thorough training on the subject and should set priorities so as to achieve greater effectiveness, so that perpetrators are successfully prosecuted and the proceeds of crime are confiscated. Particular emphasis should be placed on detection in the case of ML that could be related to cross-border transportation, precious metals and diamonds, and international or predominantly international ML cases.
- Co-ordination between the various partners in the criminal justice system should be increased.
- Reliable, comprehensive statistical data should be collected so that they may be used as tools for establishing an appropriate criminal justice policy. They should also be suitable for assessing the effectiveness of criminal prosecution and for making any necessary changes to the system.

Confiscation (Immediate Outcome 8)

- The authorities responsible for seizures and confiscations should be made aware of the importance and priority of confiscating all the proceeds of crime.
- The OCSC's central role in seizure and confiscation should be reinforced as regards both asset management and recovery.
- The Belgian authorities should implement the legal provisions passed to strengthen the confiscation of the proceeds and instrumentalities of ML and predicate offences (Law of 11 February 2014), whether they are located in Belgium or abroad, particularly by carrying out systematic financial investigations and ordering all measures aimed at the successful conclusion of confiscation proceedings. The role of the special judges responsible for enforcement investigations in criminal cases should be clarified.
- Relevant and clear statistics should be held centrally for seizures and confiscations of assets in Belgium and abroad, asset sharing, the offences in which the seizures or confiscations originated (ML and the predicate offences), confiscations related to false disclosures or false declarations at

borders, and the amounts returned to victims, so that any necessary adjustments to criminal justice policy can be determined.

3

Bibliography

CTIF (2013), *White paper on criminal money 20 years of combating money laundering and terrorist financing*, CTIF, Brussels, www.ctif-cfi.be/website/images/EN/annual_report/20yearsctifcfi.pdf

FATF (2005), *Third Round Mutual Evaluation Report of Belgium*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Belgium%20full%20FRE.pdf (in French only)

OECD (2013), *Phase 3 Report on Implementing the OECD Anti-Bribery Convention in Belgium*, OECD Paris, www.oecd.org/daf/anti-bribery/BelgiumPhase3ReportEN.pdf

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings

Suppressing the financing of terrorism

- Activities linked to terrorism and its financing, including the use of NPOs for TF, are subject to investigations and prosecutions commensurate with the risks that Belgium currently runs. Investigations into terrorism also cover TF aspects.
- Co-operation between the different authorities responsible for countering TF is commensurate with the situation and the risks that Belgium currently faces.
- NPOs as a sector have not been made sufficiently aware of TF phenomena and risks.

Application of targeted financial sanctions

- The targeted financial sanctions provided in United Nations Security Council Resolutions (UNSCR) regarding TF and financing the proliferation of weapons of mass destruction (PF) are not applied as prescribed in the FATF Recommendations, particularly in terms of time scales. Belgium has neither made nor received a request under UNSCR 1373.
- In practice, few assets have been frozen in connection with TF or PF.
- Mechanisms and initiatives are in place to inform the private sector of designations. Although targeted financial sanctions appear to be respected in Belgium, no specific measure has been put in place to monitor how well financial institutions and designated non-financial businesses and professions fulfil their obligations regarding targeted financial sanctions in connection with PF.

4.1 Context

4.1. There is a risk of TF in Belgium, even if it is difficult to measure and quantify, given the particular nature of the offence of TF and that of terrorism, to which it is inextricably linked. The majority of the structural and contextual elements influencing both the volume and types of common crime as well as the threats and vulnerabilities relating to ML, as described in this report, also apply, all other things being equal, to terrorism and TF.

4.2. According to information provided to the evaluation team, it appears that terrorist groups and individuals present in Belgium are active mainly in recruiting and collecting funds in Belgium in connection with jihadist movements in countries in the Near and Middle East (see Section 1). Links with presumed terrorist groups in Africa and the Caucasus have also been detected.

4.3. The offence of **terrorist financing** is covered in Art. 140 para. 1 and 141 of the Belgian PC (adopted in 2004). In Art.140, TF is considered as participation in an activity of a terrorist group (referred to in Art.139 PC); and Art.141 criminalises acts committed by a person who, outside the circumstances provided in Art.140, provides material resources with a view to committing a terrorist offence (referred to in Art.137 PC).

4.4. Implementing **targeted financial sanctions aimed at TF and PF** in Belgium is based on the European legal framework provided in Reg. 881/2002 and Reg. 753/2011 (for UNSCR 1267), 2580/2001 (for UNSCR 1373), Reg. 329/2007 (for UNSCR 1718) and Reg. 267/2012 (for UNSCR 1737). Belgium has also taken measures to supplement the legal framework at national level in the area of TF (RD of 28 December 2006).

4.5. In practical terms, the Federal Prosecutor's Office prosecutes all cases of terrorism and TF, and conducts the related investigations. There are also thirteen investigating judges (*juges d' instruction*) who are specialists in this area, and dedicated sections in the police forces and intelligence services. Thus the combatting of terrorism and TF suffers less from the structural problems related to lack of resources in the Belgian legal system.

Table 4.1. Cases involving terrorism prosecuted by the Federal Prosecutor's Office

2008	2009	2010	2011	2012	2013
53	52	65	84	60	150

Source: Statistics from the Federal Prosecutor's Office, 2005-2013

Note: The figures above are for cases prosecuted by the terrorism section of the Federal Prosecutor's Office and not simply those related to offences under Art. 140 and 141 of the Penal Code, but all the investigations had a financial aspect.

4.6. The Belgian authorities explained that the significant increase in cases in 2013 was due to cases linked to terrorist movements in the Near and Middle East.

4.2 Technical compliance (R 5 – R 8)

Recommendation 5 - Terrorist financing offence

4.7. **Belgium is largely compliant with R 5** – While the criminalisation of TF in Belgium responds largely to the requirements in the UN Convention and R 5, there are some technical shortcomings. Financing one or two terrorists with no proven link to one or more specific terrorist acts is not covered by the current definition. The financial penalty of EUR 30 000 is low and its dissuasiveness is in doubt.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

4.8. **Belgium is partially compliant with R 6** – The implementation of R 6 in Belgium is based principally on the EU legal framework. The UN definitions of persons in UNSCR 1988 (relating to the Taliban) and 1989 (relating to al-Qaida) have been transposed into the EU legal framework in Reg. 881/2002 and Reg. 753/2011. Nevertheless, there is a major loophole in the transposition because the mechanism cannot be applied *without delay*, as defined by the FATF. The requirement to freeze assets provided in UNSCR 1373 is implemented at European level by Reg. 2580/2001, supplemented at national level by the RD of 28 December 2006. However, there is no clear procedure allowing other countries to require Belgium to freeze assets in connection with UNSCR 1373.

Recommendation 7 – Targeted financial sanctions related to proliferation

4.9. **Belgium is partially compliant with R 7** – The implementation of R 7 in Belgium is based principally on the EU legal framework. UNSCR 1718 (relating to the Democratic People’s Republic of Korea [DPRK]) and UNSCR 1737 (relating to Iran) have been transposed into European law in Reg. 329/2007 and Reg. 267/2012, respectively. The delay in transposing the UN requirements into European law is a major loophole in the provision, since the ability to freeze the relevant assets *without delay* is fundamental to the system of targeted financial sanctions.

Recommendation 8 – Non-profit organizations

4.10. **Belgium is partly compliant with R 8** – There are shortcomings in the initiatives to inform and raise the awareness of the NPO sector to TF risks. Measures are in place to ensure their transparency, but the supervision of such organisations throughout their existence does not cover all the elements required under R 8. In addition, the nature of ‘proportionate’ sanctions has yet to be established.

4.3 Effectiveness: Immediate Outcome 9 (TF Investigation and Prosecution)*(a) Risks of terrorist financing*

4.11. An initial document entitled *Assessing the threat, risks and vulnerabilities in terrorist financing* was finalised by the competent authorities in February 2014. The document is based largely on the conclusions from the national ML risk assessment for ML (see Section 2). It was prepared on the basis of various sources and from the accumulated knowledge of several of the authorities responsible for countering the terrorist threat. The Belgian authorities indicated that this assessment identifies a number of different risks and typologies and still must be completed and updated (part of the analysis uses information from the OCAM dating from 2011, compiled for the Snapshot of police security 2012-2015 included in the National Security Plan 2012-2015).

4.12. During the evaluation team’s on-site visit, the Belgian authorities indicated that they were focussing their efforts on the terrorist risks associated with certain developments that Belgium was facing, especially in relation to the growing problem of Belgian or Belgian-resident *jihadists* and their return from conflict zones.

4.13. The actions and legal proceedings used to counter terrorism and its financing, as described by the judicial authorities, the State Security Service and OCAM, seem commensurate to the currently identified risks, even though Belgium could not provide the assessors with a full and comprehensive TF risk profile for the country.

(b) Detecting, investigating and prosecuting terrorist financing

4.14. The Belgian authorities at all levels (intelligence, the police and the legal system) take focused action against terrorist activities and those who support them, especially in the allocation of financial resources. The Belgian authorities have carried out few investigations dealing with uniquely TF offences (as an offence by itself, that is, cases where only the aspects of ‘collecting, amassing and providing funds to a terrorist group’

are involved) which were later subject to criminal prosecution. This results from the situation ‘on the ground’. Terrorists (groups and individuals) that have been subject to criminal investigation have not been involved in activities restricted simply to amassing and dispensing financial resources. Among the case studies presented by Belgium, one example from 2010 might be quoted as representative: The convictions targeted the leaders and members of a terrorist group; some of these persons had simply supported the group financially or materially. Most were convicted (one of the accused was acquitted for lack of evidence of intention). It should also be noted that the technical shortcomings in the criminalisation of TF compared with the international standard (see TC Annex, C.5.2.b)) would not have any consequences in practice. The authorities consider that the provisions in the Belgian Penal Code allow them to carry out their functions.

4

4.15. **The intelligence services (civil and military), the police forces and the CTIF work to identify terrorist activities and terrorist financing**, although the CTIF seems to produce few suspicious-transaction reports (around 20 per year). According to the authorities interviewed, this number is due partly to the fact that terrorists and their supporters use informal and parallel financial systems such as the *hawala*, and also cash on a large scale. They also make a variety of apparently legitimate transactions, particularly in the markets for used vehicles and precious metals. Other groups are financed almost exclusively by the proceeds of crime (e.g. financing by theft, robbery, extortion). Several cases described by the Belgian authorities share this feature, even if the boundary between TF and organised crime is not always easy to identify. Similarly, the people and countries involved make it difficult to determine with certainty that movement of suspect or irregular money has been used, in whole or in part, for TF or other illegal (or even legal) purposes. Lastly, the authorities have stated that in some cases, terrorist groups appear to be abusing existing NPOs or fictitious ones with reputedly humanitarian aims. In these cases, the investigations focus on those collecting funds, since if someone makes a donation without necessarily knowing the real destination of the money, the element of intention is missing. The amounts are also insignificant (sometimes donations of only a few euros).

4.16. **The competent authorities systematically analyse the financial aspect of terrorist activities** when investigating the activities of terrorist groups or individuals (for instance, how the group’s terrorist and other activities are financed, or their incoming and outgoing flows). They use all the means of investigation open to them, including requesting banking information, bugging, phone tapping, searches and observation. The same authorities may also, if necessary, seek support from the CTIF for these investigations, although at present there is little interaction as regards TF. This is due mainly to the relatively small amounts involved in some cases, but is also related to the source of the case, i.e. how the existence of terrorist activities was reported to the judicial authorities. The CTIF transmits only a few STRs on this type of case.

4.17. Where prosecution for TF is not possible, for instance when some of the elements comprising the offence cannot (or only with great difficulty) be proved (e.g. the intentional element or participation in a terrorist group), some representatives of the authorities interviewed indicated that they prosecuted based on evidence of ML.

4.18. The Belgian authorities’ significant use of international co-operation channels is discussed in Section 8. In particular, the authorities note **good co-operation with the authorities in countries bordering Belgium**. In general, international co-operation works very well in countering terrorism and TF. Requests for mutual legal assistance in order to obtain information or even evidence, including through hearings, and requests for extradition or surrender (European arrest warrant) are made regularly. International police co-operation is also used in these cases. It should nevertheless be noted that when funds are sent to or within countries experiencing regional conflicts or political instability, there are sometimes problems with co-operation in locating information and documents.

4.19. The Belgian authorities have recognised a lack of human **resources** within the State Security Service and in some services of the Federal Police (for instance, the TF Unit, which is responsible for analysing such phenomena, has just two people). The same observations cannot be made regarding investigators in the field, who are drawn from specialist police divisions. On the other hand, the judicial information system is considered outdated and inadequate for magistrates’ needs. These two factors have a negative impact on effectiveness.

4.20. The **shortcomings** noted in Section 3 regarding the length of procedures (due largely to congestion in the courts and, to a lesser degree, the misuse of some appeal procedures, all things being equal) apply to some extent to countering TF.

4.21. These aspects are partly counterbalanced by the good **collaboration** between the authorities responsible for countering terrorism and its financing. There are specialised units with unquestioned commitment and expertise within the Federal Prosecutor's Office, specialised investigating offices, the intelligence services and the police forces.

(c) Sanctions

4.22. Based on the information received by the assessors, the penalties imposed on those found guilty of TF offences appear proportionate, given that the convictions cover terrorist financing together with other offences.

4.23. The Belgian authorities indicated that **to date there have been four convictions in Belgium for TF as the sole offence**. There have also been a number of convictions for TF as one of the elements accepted as participation in a terrorist group (e.g. Brussels 2010, Brussels 2014). Several people have been acquitted. No legal person has currently been convicted of TF in Belgium.

4.24. As to whether the penalties provided and imposed for offences under Art. 140 and 141 of the Penal Code are effective and dissuasive, the Belgian authorities indicated that the sentences handed down under Art.140 vary from a suspended prison sentence of several months to one of several years - up to 20 in one case - and that they are thus significant and certainly dissuasive. When deciding the length of sentence, the courts take into account the criminal record of the convicted person and the likelihood he/she has of being re-integrated into Belgian society. Sentences also regularly include fines and confiscation, as well as extradition. In all cases, an appraisal of the dissuasiveness and effectiveness of the sanctions for TF must take into account the ideology and the degree of indoctrination of some terrorist organisations.

(d) Other measures

4.25. As regards alternative means of combatting TF (i.e. other than criminal prosecution), the Belgian authorities have defined two avenues for mitigating the risks of TF: (i) an administrative authorisation must be obtained from the municipal authorities when funds are collected from the public (controlling to some extent the raising of funds by NPOs); and (ii) natural persons known or assumed to have left national territory for certain combat areas are struck from the register, to prevent welfare grants or allowances being subverted for the purposes of TF. The Belgian authorities have thus refused to renew one person's residence permit and started legal proceedings to withdraw Belgian nationality (for those with dual nationality).

4.26. The Federal Prosecutor's Office, together with the other authorities and agencies dealing with this threat, prepare what are known as 'concept cases'. The aim is to optimise co-operation, co-ordination and information exchange between authorities at federal, local and also European level, and to ensure that the relevant criminal policy is constantly adapted to the threats and typologies encountered.

4.27. **In conclusion**, the tactics and methods used by the Belgian authorities are not exclusively oriented towards the financing aspects of the global terrorist threat, but nothing in the actions that they undertake or in the court judgements that the assessors were able to review indicates that the Belgian authorities are negligent in countering TF. Based on the information provided to the assessors and interviews with the specialists involved, it appears that **the action of the Belgian authorities is commensurate with the actual phenomena and threats**; they are detecting offences and participating actively in countering terrorism. People have been convicted for TF in cases that cover terrorism more broadly.

4.28. **Belgium has achieved a substantial level of effectiveness for Immediate Outcome 9.**

4.4 Effectiveness: Immediate Outcome 10 (Preventive Measures and Financial Sanctions relating to TF)

(a) Targeted financial sanctions

4.29. As regards the implementation of targeted financial sanctions, as was stated in more detail when discussing technical compliance (R 6), the UNSCR 1267 and subsequent resolutions are not implemented in a way that complies with the FATF Recommendations, in particular because the EU's transposition system is too slow to ensure that assets are frozen *without delay* (as defined by the FATF) and no other Belgian measure compensates for it. The mechanism of the so-called 'Belgian' list, provided in the RD of 28 December 2006 to enable Belgium to apply sanctions to persons not (yet) designated at European level, has not yet been implemented. Its effectiveness is thus unproven (at the time of the on-site visit, the Belgian authorities stated that an initial list was being compiled). These delays cast doubt on the ability of the Belgian authorities to freeze rapidly (and effectively) the assets of persons or entities targeted by the UN, and have also a negative impact on the effectiveness of action by the Belgian authorities.

4.30. In practice, few assets have been frozen: one building and one bank account were frozen in 2002 (and still are) under UNSCR 1267. Furthermore, no designation request under UNSCR 1373 has been made either to or by Belgium.

4.31. The mechanism for informing the private sector about listed persons is rather passive (organisations are required to consult the EU Official Journal, the Belgian Official Gazette [*Moniteur belge*] and the web sites of the competent authorities). The CTIF and FPS Finance (see R 6, C.6.5.d) have nevertheless published guidelines for financial institutions and the DNFBPs on their obligations in this matter. A CBFA circular simply reminds financial institutions of their legal obligations in this regard (see R 6, C.6.5.d). FPS Finance claims that the private sector informs itself, in particular by consulting databases established by certain private companies (apart from consulting regularly the official, and in particular the European, lists). This was confirmed by the finance sector representatives met with, who are not afraid to contact the CTIF or the FPS Foreign Affairs in case of doubt (see Section 5.3.d). The BNB and the FSMA check that the financial institutions have implemented an appropriate system or internal procedures to apply the targeted financial measures. The way in which DNFBPs (apart from lawyers) are made aware firstly of the mechanisms for targeted financial sanctions and the measures to take, and secondly of the lists to consult and controls to apply, appears inadequate (see Section 6.3.b).

(b) Non-profit organizations (NPOs)

4.32. **The authorities describe part of the NPO sector as presenting a risk of TF** (foundations, on the other hand, do not appear to be a sector at risk in terms of terrorism). Thus the plan on radicalisation (or *Plan R*) from OCAM has since 2005 aimed to detect and monitor radical individuals, groups and media, and includes aspects of TF. The non-profit associations (*associations à but non lucratif - ASBL*) in question either are directly involved because they support certain organisations considered terrorist that are active in the Near and Middle East, with parallel activities (such as education or medical aid); or have no link to terrorist groups but are used by some members to collect funds, sometimes without even the administrators of the organisation being aware of it (see IO 9). There have been no significant actions, either targeted or routine, to impose administrative controls on associations. The sector is supervised for tax purposes because of the special features of associations in this sector (see R 8, C.8.3); however, the NPOs at risk are smaller. Nevertheless, these same authorities consider that the risk of TF related to NPOs has diminished over the last few years (fund raising and events during which money may be collected must be authorised by the authorities). The risk has shifted, partly because terrorists and their financiers are using alternative methods (*hawala*, for instance) or are raising funds by trading some types of goods.

4.33. The representatives from associations interviewed during the on-site visit (from major Belgian non-profit associations) did not seem to be aware of, or even sometimes to understand, the risks of the misuse of NPOs for TF purposes. Although aware of the risks of fraud in unauthorised fund raising, they did not appreciate the reasons why a terrorist organisation might be drawn to create an association. Thus the action taken to raise the sector's awareness is not sufficient (see R 8, C.8.2).

4.34. **The National Security Service monitors in particular the activities of certain NPOs** that could be used by terrorists, and the CTIF sometimes receives STRs involving small associations. Between 2005 and 2010, the Federal Prosecutor's Office undertook a 'proactive' investigation¹ of a list of ASBLs for which there were reasonable suspicions of TF. The investigation succeeded in particular in developing with the court districts concerned a policy supervising the strict application of the law on associations, and resulted in certain NPOs being wound up or normalised. The investigation has not been repeated: although the authorities indicated that they would like to carry out similar investigations, they do not have the necessary human and financial resources.

4.35. **In conclusion**, Belgium has a legal system in place to apply targeted financial sanctions regarding terrorist financing. However, given the technical shortcomings identified (particularly the time scales for applying new sanctions), the effectiveness of the Belgian system is questionable. In practice, very few assets are frozen, although this is not in itself an indicator of inefficiency, as it has not been established that the assets targeted by the sanctions are on Belgian soil.

4.36. Regarding the risk of NPOs being used for terrorist purposes or for TF, there are shortcomings in the administrative controls or transparency requirements for NPOs, awareness raising and targeted actions, but the Belgian authorities have identified the NPOs at risk and monitor continuously their activities and transactions.

4.37. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 10.**

4.5 Effectiveness: Immediate Outcome 11 (TFS relating to PF)

4.38. An effective system of financial sanctions regarding proliferation depends on the immediate implementation of the UNSCRs, monitoring compliance with the measures imposed, co-ordinated action by the authorities concerned to prevent the measures being circumvented and preventive action. **Belgium does not implement without delay** (as required under FATF Recommendation 7) **the targeted financial sanctions** defined in the UNSCRs relating to combatting PF. The implementation of targeted financial sanctions for PF in Belgium are based on the European legal framework set out in Regulation 329/2007 (for UNSCR 1718 concerning the Democratic People's Republic of Korea – DPRK) and 267/2012 (for UNSCR 1737 concerning the Islamic Republic of Iran). These measures apply freezing measures to a broad range of funds and property. These mechanisms suffer from technical problems in the length of time for transposition (see TC Annex, R 7). In practice, delays have been noted in the publication of designated names by the EU, as regards both Iran and the DPRK.²

4.39. The Belgian authorities do not contest that the transposition system is too slow, but say that the problem is largely mitigated by the preventive measures applied by the financial institutions and the DNFBPs. In fact, given the particular nature of the subject and the countries concerned, the private sector – especially banks and insurance companies – are both aware and watchful. Here too, the private sector confirms that it keeps abreast of UN decisions by itself consulting certain web sites, without waiting for transposition into European law. Any transaction would immediately prompt an alert. No violations of the obligations

1 A 'proactive' investigation consists of looking for, gathering, recording and processing data and information based on a reasonable suspicion that criminal acts will be, or have been, committed but are not yet known. It is allowed for a list of offences including terrorism and its financing (Art. 28bis and 90ter CPC).

2 Iran: Reg.522/2013 (implementing Reg.267/2012) was adopted on 6 June 2013 to incorporate a change decided by the Security Council on 20 December 2012.

DPRK: On 2 May 2012, the Sanctions Committee decided to add three names to the UN sanctions list. Four more names were added to the same list on 22 January 2013. Reg.137/2013, including these names on the European list, was adopted only on 18 February 2013.

regarding targeted financial sanctions were found. The Belgian authorities consider the risk of damage to financial institutions' reputation to be high, and this motivates them to comply with these obligations. For other economic players, the UN's system of designations and sanctions **may appear complex**, and many tend to adopt a conservative attitude for fear of violating the law. There are, at present, no or practically no business relationships or commercial transactions with the targeted countries.³ This conservative attitude, although it may be effective, has a negative impact on legitimate transactions (a problem related to *de-risking*). The problem of time scales is also considered to be mitigated because the EU applies sanctions to a significant number of entities that are not designated by the UN, and uses a prior-authorisation procedure for transactions with Iranian organisations, so that any transaction initiated can be delayed while European transposition is in progress (see above).

4

4.40. The Belgian authorities consider that even if the UNSCRs are not immediately formally transposed, there is only a very low probability that the delay will affect the effectiveness of targeted sanctions. This remains to be confirmed however, since assets located in Belgium could be used in indirect transactions (that is, with the participation of a third country or persons that have not been designated). In addition, the system for declaring and pre-authorising transactions does not have an impact on assets already located in Belgium that have not been involved in transactions. These measures, despite their positive effect, do not alone satisfy the requirements to identify and deprive the resources of designated persons *without delay*.

4.41. The low risk and conservative attitude of certain players cannot alone be taken as a measure of the effectiveness of a national strategy to prevent and disrupt PF. Such a strategy also requires a robust system for monitoring and supervising financial institutions and DNFBPs as regards their obligations relating to targeted financial sanctions for PF. Although the Belgian authorities seem confident that the private sector applies measures, **they have not been able to supply conclusive evidence that controls have been in place over the last few years**. If the supervisors of financial institutions make sure that institutions have procedures and systems for monitoring FP designation lists, they do not determine whether the systems are implemented effectively. For example, no information was provided on the identification and management of false-positives, a problem that often comes up in an effective system. Moreover, it falls to the police and AGDA to check whether targeted financial sanctions are observed, and checks are made only in the case of a suspected violation (no checks will have taken place). Checks for DNFBPs were not confirmed in this area. It is not possible to decide with certainty why assets frozen under the UNSCR have a low value: the system may be ineffective, or there may be little PF in Belgium.

4.42. **In practice, the amount of frozen funds is rather low** (less than EUR 500 000 for a half dozen accounts). All of these freezing measures concern Iran (there were none for DPRK) for entities designated by the UN or the EU. There was no request for authorisation to access these accounts which were not used in practice.

4.43. Belgium is implementing additional measures in order to prevent proliferation financing and to frustrate attempts to circumvent targeted financial sanctions. Firstly, to ensure compliance with the measures decided by the UN and the EU Council, the National Security Service carries out activities to raise awareness among private businesses and operators. The CTIF also included in its December 2013 Guidelines (for institutions and persons covered by the law) guidance on reporting suspected PF in relation to Iran and the DPRK.⁴

4.44. A prior authorisation from FPS Finance (Treasury Administration) is required to carry out certain transactions (exceeding different thresholds depending on the country concerned) with persons or entities associated with the targeted countries. FPS Finance has processed about 2 500 authorisation requests for

3 According to the statistics on Belgian foreign trade published by the BNB, Belgium exported goods to Iran with a total value (in EUR) of: 271 million in 2009, 369 million in 2010, 364 million in 2011, 198 million in 2012 and 141 million in 2013. Imports from Iran amounted to 86 million in 2009, 104 million in 2010, 89 million in 2011, 21 million in 2012 and 13 million in 2013. There are no exports to or imports from the DPRK.

4 CTIF/CFI (2013), p.25 et s.

Iran, and only around ten have been refused. The Belgian authorities consider that the rate is low because those asking are well informed, and anticipate possible refusals. The Belgian authorities indicated that when FPS Finance gives an authorisation, it informs the UN Security Council as to whether or not the European transposition has taken place. There is also a system for **reporting** particular transactions (for instance, any transaction with Iran over EUR 10 000). Representatives from the financial sector indicated that it was proving difficult to apply enhanced due diligence to the rules on embargoes because the measures were complex and some points required interpretation; and that they would welcome more information. Nevertheless, several STRs dating from 2010 were mentioned, as was a recent CTIF file, which could not be discussed because no decision has yet been made to send it to the judicial authorities. In all, the CTIF has sent several PF-related files to the judicial authorities.

4.45. The State Security Service (SE) and military intelligence (SGRS) play the leading role in countering PF, although the work of FPS Finance and the AGDA should not be understated. The assessors noted the **good co-operation** and co-ordination knowledge of the authorities responsible for combatting this activity, at all levels (regional and federal), and PF is integrated into combatting proliferation. These services also collaborate closely with their foreign counterparts in particular cases (cf. IO 1, chap. 2.3.e).

4.46. **In conclusion**, the Belgian legal system, in conjunction with that of the EU, enables the implementation of UNSCRs relating to targeted financial sanctions to combat PF, but the transposition time scales we observed have a negative impact on the system's effectiveness. Information should be disseminated rapidly, and beyond major financial businesses, even before transposition into European and thus Belgian law; training is needed for all sectors covered by the AML/CFT Law. Checks have not been implemented effectively as to whether obligations relating to targeted financial sanctions for PF are being observed. The actions undertaken to frustrate attempts to circumvent the sanctions regime show that the various competent authorities have the expertise and are knowledgeable in the relevant areas, although it is regrettable that the financial aspect of proliferation is not more emphasised.

4.47. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 11.**

4.6 Recommendations on terrorist financing and proliferation financing

Investigating and prosecuting terrorist financing (Immediate Outcome 9)

- Belgium should consider allocating more resources, both human and IT, to the services responsible for countering terrorism and its financing, to enable a more proactive approach.
- The Belgian investigation and prosecution authorities should regularly reassess their approach to TF as an offence incidental to terrorism, based on changes in patterns of risk; and continue systematically to analyse the financial aspect of terrorist cases.
- Belgium should update its analysis of TF risks and deepen the risk analysis completed in February 2014: it should contain a more detailed profile of risks and strategy for TF.

Targeted financial sanctions on terrorist financing (Immediate Outcome 10)

- Belgium should implement the RD of 28 December 2006 in order to temporarily freeze the assets of persons designated under UNSCR 1267, while waiting for UN decisions to be transposed into decisions of the EU Council.
- Belgium should plan to fully implement the system for freezing assets at national level by publishing a list of designated names in the context of the RD of 28 December 2006.
- Belgium should ensure that DNFBDs are more aware both of the difference between the lists of high-risk countries and the lists of persons and organisations that are subject to targeted financial sanctions; and of the measures to adopt in the presence of customers appearing on these lists.

- Belgium should take action to raise NPOs' awareness of possible misuse of their organisations for TF purposes, and the enforcement authorities should periodically monitor NPOs which are reasonably suspected of TF.

Targeted financial sanctions on the financing of proliferation (Immediate Outcome 11)

- Belgium should enable targeted financial sanctions relating to PF to be implemented *without delay*, as required by the FATF Recommendations. Belgium should establish a system enabling assets of persons designated under UNSCRs 1718 and 1737 to be frozen temporarily, while waiting for UN decisions to be transposed into decisions of the EU Council.
- Belgium should enhance the mechanisms for informing the financial sector and the DNFBPs of targeted financial sanctions related to PF, to ensure that all players fully understand their obligations.
- Belgium should implement controls checking compliance with the obligations relating to targeted financial sanctions for PF.

4

Bibliography

CTIF/CFI (2013), Ligne directrice destinée aux organismes et personnes visés aux articles 2, §1, 3 et 4 de la loi du 11 janvier 993, CTIF/CFI, Brussels, www.ctif-cfi.be/website/images/FR/ld121220132.pdf.

5. PREVENTIVE MEASURES

Key Findings

Understanding of AML/CFT risks and obligations

- The financial institutions we met generally seemed to have a good understanding of the risks, including the banks dealing with the diamond trade, Bpost and the new entrants in the financial sector (payment institutions and electronic money institutions). Money remittance institutions also seem to understand the risks of TF and misuse to which they are exposed.
- Generally, the DNFBPs do not seem to have grasped the full extent of the ML/TF risks to which they are exposed, nor the need to protect themselves against potential ML/TF misuse.
- Regarding the diamond trade, while the sector acknowledges that the risks are high, it considers that the existence of strict, stringent AML/CFT measures is a key risk-mitigation factor. However, the implementation of the existing rules does not appear to be sufficiently rigorous, on the whole, to ensure that these high risks are effectively controlled.
- Most financial institutions have a good understanding of AML/CFT obligations. However, certain payment institutions and certain bureaux de change have a patchy understanding of the requirements concerning beneficial owners and politically exposed persons (PEPs).

Implementation of the preventive measures

- Customer due diligence measures (CDD) and ongoing due diligence measures on transactions would appear to form the foundation of the AML/CFT system for the financial and non-financial institutions interviewed.
- Institutions in the financial sector generally seem to implement proportionate AML/CFT measures and adopt appropriate measures based on the risks. The financial sector generally seems to implement enhanced due diligence measures in recognised high-risk situations, though to a lesser extent for correspondent banking relationships and wire transfers within the EU.
- While DNFBPs seem to have understood the need to take enhanced measures when handling a transaction or customer involving a higher-risk country, they seem to be less aware of this necessity for PEPs and the other situations requiring close attention. When DNFBPs are unable to meet CDD requirements, they indicated that they decline to enter into a business relationship or carry out a transaction, even if they do not send in an STR.
- Closer AML/CFT supervision by the competent authorities is necessary to ensure that those subject to the AML/CFT Law fulfil their obligations appropriately.

Suspicious transaction reporting

- The financial sector has, on the whole, adopted the practice of STR. Even so, the activities of the bureau de change sector and payment transactions carried out by institutions through a network of agents give rise to a significant proportion of automatic STRs, which are not useful for following the transactions of customers who have already been reported. A strengthening of controls in this area is necessary.
- The DNFBPs under the requirement to report transactions on the basis of thresholds/criteria (casinos in particular) often limit themselves to this type of 'objective' reporting and do not report based on an assessment of the suspicion arising from transactions carried out. Notaries and the accounting/tax professions nevertheless seem to take 'subjective' factors into account when deciding whether or not to report suspicious transactions. There are still virtually no STRs from lawyers and diamond traders. This approach may lessen the ability to detect ML and result in an under-representation of certain phenomena in criminal prosecution.

5.1 Background and Context

(a) Financial institutions and DNFBPs¹

5.1. *Financial institutions* - Belgium has **104 credit institutions**, including 55 branches of institutions based in the European Economic Area (EEA).² There are also 676 financial institutions declared as operating under the *freedom to provide services* on the basis of the European passport, which allows licensed institutions from one Member State of the EEA to offer their services in another Member State without being established there. At end of 2012, the country's five largest banks held 66.3% of the total assets of all of the banks combined, and three of them were Belgian subsidiaries of foreign groups. The ML/TF risks to which the Belgian banking sector is exposed stem more specifically from the types of transactions performed for their customers (payments/deposits, money remittances) and their international relations. Belgium also has banks specialised in financing the diamond industry: primarily three major European stakeholders (one of which operates out of London), and branches of smaller Indian banks. These banks are exposed to more specific ML/TF risks associated with their customers' business activities (see below).

5.2. Most of the financial activities subject to the AML/CFT system are conducted in banking groups. Investment services are also offered by 20 brokerage firms, 7 management companies for collective investment funds and 19 investment management and investment advisory companies. For the latter two categories, customers' assets are always held by another institution (a bank or brokerage firm) and the company provides only management or consulting services, so there are no asset transfers and less risk of ML/TF. Even so, there may still be risks associated with the source of the funds. Some of these companies also offer a service for receiving and issuing stock exchange orders, but it never includes asset transfers, which have to be carried out and liquidated by a bank or a brokerage firm. There are also 530 Belgian and foreign management companies for collective investment schemes. The only cases in which there may be a ML/TF risk involve open collective investment schemes (i.e. with a variable number of shares). In practice, this risk is covered because all of the open, self-managed collective investment schemes have delegated the marketing of their shares to a brokerage firm or credit institution (which are subject to AML/CFT controls).

5.3. **Mortgage credits** are mainly distributed by credit institutions. Belgium has 127 independent mortgage credit companies, most of which play a social welfare role for small loans at conditions set by the public authority. Additionally, these companies are not allowed to collect public deposits, so present a lower risk of ML/TF. Belgium also has around 50 **finance leasing** companies and 85 **consumer credit** companies, most of which also belong to banking groups.

5.4. Belgium has 23 **life insurance** companies and 24 endowment insurance companies, as well as 275 operators acting under *freedom to provide service* provisions. There are also 9,326 **intermediaries** registered in the life insurance branches (brokers and non-exclusive agents), but who are not all active in this branch. The majority of life insurance contracts are concluded directly with insurance companies (in 2012, brokers accounted for 23.5% and agents for 4.8%). The characteristics of life insurance contracts (e.g. the need to identify the insured, an identifiable beneficiary, the method for collecting the premium and paying out the capital) and the detailed typology of ML/TF risk factors (e.g. surrendering premiums shortly after concluding the contract for no valid reason and involving heavy financial losses, operations resulting in the loss of a sizeable tax advantage, etc.) mean that the ML/TF risks identified for these products are lower in Belgium.

5.5. There are 12 **bureaux de change**. Since 2011, bureau de change registration covers only the spot foreign exchange business and physical money changing. A number of businesses have accordingly opted

1 The figures shown in this section were issued by the Belgian authorities and are available here: BNB (2013); BNB website (http://nbb.be/pub/cp/domains/psd/li/psd3_li.htm?l=fr&id=psd3); FSMA (2014); FSMA website (www.fsma.be/fr/Supervision/finbem/bo/Article/lijsten/bo1.aspx); Febelfin (2014a); Assuralia (2014).

2 The European Economic Area is an economic union formed of the EU Member States and the countries belonging to the European Free Trade Association (EFTA) – Iceland, Liechtenstein, Norway and Switzerland. The provisions governing the EU's internal market apply also to the EFTA countries.

PREVENTIVE MEASURES

for the status of payment institution, which allows them to provide payment services, including **money remittance services**. Belgium has a total of 236 payment institutions, including 17 European institutions operating under freedom of establishment through 1 473 agents based in Belgium. A major European payment institution concluded an agreement with Bpost (see below) to offer a money remittance service through the network of post office counters and its 700 public sales outlets. In Belgium there are also **nearly 270 institutions offering a money remittance service and operating under freedom to provide services; most of these services come from the United Kingdom**.

5.6. The total value of money transfers in Belgium amounted to EUR 490 million in 2012, with most going to non-European countries, mainly Morocco, Turkey and the Democratic Republic of Congo.³ The risks associated with these transactions and with money and currency changing remain high because of the proportion of cash used.

5

5.7. There are 50 **electronic money** institutions, including 10 institutions governed by Belgian law, one European institution operating through distributors and 39 operators doing business under *freedom to provide services*.

5.8. **Bpost** is also specifically targeted by the AML/CFT system. This public limited company, the primary business of which is providing postal services, also offers financial services through the postal network.⁴ It conducts business activities on its own behalf, some of them as part of its public service missions (postal current accounts, postal remittances, national postal money orders, etc.), in addition to the sale of 'bpaid' prepaid cards. It also conducts business activities on behalf of third parties, including a money remittance service as an agent for a European payment institution (see above). These money transfers, most of which are international, amounted to a total of EUR 317 772 000 in 2013, with an average value of EUR 326.

5.9. *Designated non-financial businesses and professions (DNFBPs)* – Belgium has 1 505 **notaries** working in 1 072 notary offices. Notaries are public officers who hold a monopoly for the establishment of authentic instruments in relation to real estate property transfers and the incorporation of legal persons. The 9 042 licensed and trainee **real estate agents** also play an important intermediary role in real estate transactions.⁵ These activities are potential channels for ML/TF that put these professions at risk.

5.10. The Belgian Bars record a total of 17 795 **lawyers**, but not all of them exercise activities covered by the AML/CFT system. According to the CTIF, 10% of them can be considered 'company lawyers' accordingly involved in operations pertaining to company operations and financial transactions. All of the **accounting/tax professions** included in the AML/CFT system represent 9 321 accountants and tax accountants, external chartered accountants and external tax consultants (professionals working individually and in firms); there are 1 053 statutory auditors. These professionals are involved in businesses' everyday operations and may be confronted with transactions connected to tax fraud and social security fraud (and the associated ML).

5.11. Belgium has nine **casinos**, which all hold licences to offer online casino gaming (which require the server to be based in Belgium), but only seven of them actively use this additional licence.⁶ Handling cash is one of the main ML/TF risks facing casinos.

3 Eurostat (2013); World Bank (2013).

4 A distinction must be made between Bpost and Bpost Banque, a 50% subsidiary of Bpost and a credit institution subject to BNB supervision.

5 Chartered surveyors, when they exercise the regulated activities of real estate agents, are also covered by the AML/CFT system.

6 Gaming Commission (2013).

5.12. There are nearly 1 700 **diamond traders** in Belgium, mainly in Antwerp.⁷ They include rough diamond producers and merchants, polished diamond producers and wholesalers, and the manufacturers of machines or tools that contain a diamond component (e.g. grinders and saws). Traders who only retail in diamonds are not included. These diamond traders' business is mainly based on import and export, mostly to or from EU third-party countries. Shipments of diamonds imported into Belgium or exported from a country outside the EU must be physically checked by the Diamond Office.⁸ The weight, classification and value of the diamonds are compared with the data on the invoice and trade documents by experts acting on behalf of the SPF Economy. The SPF Economy is also responsible for verifying the authenticity of Kimberley Process Certificates with the objective of stemming the flow of conflict diamonds.⁹ The international nature of the diamond trade, the large volumes traded, the value of the products and ease with which diamonds are transported are among the main factors that make this trade a business with a high risk of ML/TF.

5.13. The 9 **security firms** in Belgium authorised to provide secure transport services for high-value items are also subject to the AML/CFT regime because their business activities involve handling cash and/or other high-value items such as precious stones. The 552 **bailiffs**,¹⁰ grouped into 249 non-commercial companies (*sociétés civiles*), are also subject to AML/CFT measures because, in their task of executing judicial decisions, they may, for example, be confronted with situations in which a debtor with outstanding debts (late VAT or social security payments) offers to pay a large sum in cash, which may be a sign of laundering money from a fraudulent bankruptcy or misappropriation of corporate assets.

5.14. 'Company service provider' is not an organised, regulated business as such in Belgium, so is not covered by the AML/CFT regime. To date, Belgium considers that this profession does not exist, as such, in Belgium. The activities covered by the FATF for this category are exercised primarily by lawyers and accountants (and possibly notaries).¹¹ However it appears that in recent years, professional company domiciliation services have developed in Belgium.¹² Typologies of fraud using company domiciliation and rules on the siting of companies' head office in Belgium have also been identified. The authorities have accordingly undertaken work to regulate these activities and make them subject to AML/CFT obligations, and may consider extending these measures to trustee companies (*sociétés fiduciaires* -- accounting and tax firms) (see Section 7 also).

(b) Preventive measures

5.15. AML/CFT preventive measures are grounded in the Law of 11 January 1993 on the prevention of the use of the financial system for the purpose of ML and TF ('AML/CFT Law'). The law was amended in 2010 to transpose the third AML/CFT Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of ML and TF, and the introduction of measures arising from the FATF mutual evaluation in 2005. Substantial changes were made, mainly to the regime applicable to DNFBPs, by tightening the anti-ML/TF requirements and supervision of the professionals.

7 FATF (2013).

8 www.diamondoffice.be.

9 www.kimberleyprocess.com.

10 In Belgium, bailiffs are ministerial and public civil servants who exercise their function on a self-employed professional basis. They are in charge of issuing and enforcing decisions of justice. They are also qualified to manage amicable debt recovery, organise voluntary sales of furniture and physical household effects, carry out building administration, establish affidavits at the request of a magistrate or a private individual, and the draft rental leases and other private agreements.

11 FATF (2005), para. 592.

12 It is difficult to quantify the number of these companies. The Belgium Office Business Center Association comprises 12 companies, but FPS Economy believes the sector is in fact much larger.

PREVENTIVE MEASURES

5.16. Note that the **minimum threshold set for applying due diligence measures to occasional customers is EUR 10 000** (Art. 7 §1 2° of the AML/CFT Law), which is lower than the threshold in FATF Recommendation 10.

5.17. **Regulatory measures have been taken to apply the provisions of the law**, including the preventive obligations, to the various businesses and professions covered:

Table 5.1. Regulatory measures

Persons and institutions covered by the law	How the AML/CFT Law is applied	Authority/Authorities responsible for regulation, supervision and monitoring
Financial sector		
Credit institutions	RD of 16 March 2010 approving the CBFA Regulation of 23 February 2010 ¹	National Bank of Belgium (BNB)
Investment companies		
Clearing entities		
Insurance companies		
Payment institutions		
Electronic money institutions		
Banking and investment service brokers		Financial Services and Markets Authority (FSMA)
Insurance intermediaries		
Collective investment funds		
Collective investment fund management companies		
Investment management and investment advisory companies		
Bureaux de change		
Mortgage providers		FPS Economy
Regulated-market operators		
Consumer credit companies ²	No existing regulatory measures	
Finance leasing companies		
Bpost	Order of the Minister on 10 January 2014	FPS Finance

1. Following the reorganisation of financial sector supervision in Belgium in 2010 (see Section 6), earlier decisions by the CBFA, including circulars, remain valid (Art. 329 to 331 of the RD of 3 March 2011 [Ministry of Justice, Ministry of Finance et al, 2011]).
2. The Law of 31 July 2013 removed the provision of the Law of 2 August 2002 (Moniteur Belge / Belgisch Staatsblad, 2002) that assigned to the FSMA the role of supervising consumer credit companies and operations, with effect from a date to be set by royal decree. It was decided that FPS Economy would be charged with supervising credit regulation (mortgage and consumer credit) and that the FSMA would be charged with controlling access to the business of lenders and intermediaries in these sectors, through the Law of 19 April 2014. The section of this law related to the FSMA's competence will enter into force on 1 July 2015.

Table 5.1. Regulatory measures (continued)

Persons and institutions covered by the law	How the AML/CFT Law is applied	Authority/Authorities responsible for regulation, supervision and monitoring
Designated non-financial businesses and professions (DNFBPs)		
Real estate agents and chartered surveyors	RD of 30 July 2013 approving the regulation of FPS Economy	FPS Economy
Security companies	RD of 26 March 2014 approving the regulation of FPS Interior	FPS Interior
Diamond traders	RD of 7 October 2013 approving the regulation of FPS Economy	FPS Economy
Notaries	Regulation of the National Chamber of Notaries of 26 April 2011, amended on 18 April 2013	National Chamber of Notaries and Chamber of each of the 11 provincial companies
Bailiffs	Regulation of the National Chamber of Court Bailiffs, adopted on 27 October 2012 and amended on 16 November 2013	Belgian National Chamber of Court Bailiffs
Statutory auditors	Rule issued by the board of the IRE of 4 February 2011 ³	Institut des Réviseurs d'Entreprises (IRE)
External chartered accountants and external tax consultants	Regulation of the Institute of Chartered Accountants and Tax Consultants of 10 January and 7 February 2011	Institut des Experts comptables et des Conseils fiscaux (IEC)
Certified accountants and tax accountants	Regulation of the National Council of the Professional Institute of Certified Accountants and Tax Accountants of 28 January 2011	Institut Professionnel des Comptables et Fiscalistes Agréés (IPCF)
Lawyers	Regulation of the Order of French-speaking Bars and the German-speaking Bar of 14 November 2011. Included in the new code of professional conduct (Art. 4.68 to 4.74)	Order of the French-speaking Bars and the German-speaking Bar and each of the 14 bars
	Regulation of the Order of Flemish Bars of 21 December 2011	Order of the Flemish Bars and each of the 14 bars
Casinos	Law of 7 May 1999 and RD of 15 December 2004	Belgian Gaming Commission (FPS Justice)

3. The three institutes for the accounting/tax professions (IRE, IEC and IPCF) decided to adopt a common set of rules to allow a consistent application of the law.

5.18. The measures necessary to adjust the Belgian AML/CFT framework to the revised FATF Recommendations of 2012 have not yet been taken. The Belgian authorities indicated that, to avoid successive amendments to the legal and regulatory framework in a short lapse of time, they will make all the necessary adjustments at once, when the measures are taken to transpose into Belgian law the fourth AML/CFT Directive currently being developed.

5.19. Likewise, because the measures applicable to money transfers are governed by EC Regulation 1781/2006, they will be adjusted at the end of the legislative process under way at European level, in which Belgium is taking part, in view of adopting a new Regulation. This work intends to reflect FATF's new R 16

and thus introduce requirements regarding information about the beneficiaries of money transfers and the additional obligations for intermediary financial institutions.

(c) Risk-based exemptions or extensions of preventive measures

5.20. **Diamond merchants are the only dealers in precious stones subject** to the entire Belgian AML/CFT system. This is because these merchants handle the largest business deals, which can involve very substantial sums.¹³ Moreover, the international nature of the diamond market, the volumes traded, the ease with which the diamonds traded are transported, the key role of Antwerp in the international diamond trade, the concentration of the stakeholders and the continued existence, to a certain extent, of informal practices for concluding the deals are typical features of a sector with a high risk of ML/TF. This is corroborated by information held by the operational services (police and investigators) and ML/TF cases calling into question those involved in the diamond trade (see Section 3). In Belgium, the sector with the highest risk of ML/TF is therefore precious stones.

5.21. **Dealers in precious metals** (gold, silver and platinum) are not covered by AML/CFT preventive measures, but they are subject to the **provisions restricting cash payments** (EUR 3 000 or 10% of the total price), which also apply to any dealer or service provider (Art. 21). These requirements were introduced in 2012 to address the underground economy, ML, social security fraud and tax fraud. They were tightened in 2013, mainly in response to cases forwarded by the CTIF, which concerned transactions worth huge amounts (over EUR 1 billion) that involved purchases of old gold.

5.22. **Security companies, external tax consultants and court bailiffs** are not among the professions covered by the FATF Recommendations. However, since the Law of 10 August 1998, Belgium has deemed it necessary to include these businesses and professions in the AML/CFT system on account of their exposure to the risks of tax fraud (tax consultants) and the handling of cash (security companies and bailiffs).¹⁴

5.2 Technical compliance (R 9 to R 23)

Recommendation 9 – Financial institution secrecy laws

5.23. **Belgium is compliant with R 9** – The contractual duty of discretion between the customer and the financial institution is lifted when information must be forwarded to the judicial, tax and prudential supervision authorities, or to the CTIF.

Customer due diligence and record keeping

Recommendation 10 – Customer due diligence

5.24. **Belgium is largely compliant with R 10** – The measures provided in the AML/CFT Law meet the main requirements of R 10. Beneficial owners must be identified and their identity must be verified by taking appropriate risk-based measures defined by the financial institutions in their internal procedures. If

13 Certain lots of diamonds transiting through the Antwerp marketplace have market values of millions of euros. In 2012, the value of trade amounted to USD 51.9 billion, which represents a value of USD 200 million passing through Antwerp every day. Risk analysis of the Antwerp diamond sector, AWDC, November 2013.

14 This report did not analyse the compliance of the measures applicable to these businesses and professions, insofar as they were excluded from the scope of the Recommendations (para. 591). Even so, the new version of the Recommendations is risk-based. Insofar as Belgium considers that these sectors present a risk that it should try to avert and mitigate by applying AML/CFT measures, they are included in the sectors examined as part of this mutual evaluation.

supporting documents cannot be furnished, the financial institutions can access the National Register (of physical persons) through their industry trade group. If the information cannot be verified, the financial institution should keep a written record of the measures taken, as documentary evidence that they were appropriate for the risk involved. The limitation of the system is that the provisions applicable do not specify whether the financial institution should, by default, consider the company's senior managing official as the beneficial owner when no natural person can be identified as such in the case when the function of member of the board of directors is separate from that of 'senior managing official'. Moreover, there is no explicit provision that obliges financial institutions to systematically consider the beneficiary of a life insurance contract as a relevant risk factor when they determine whether enhanced due diligence measures should be applied.

Recommendation 11 – Record keeping

5.25. **Belgium is compliant with R 11** – All documents concerning transactions must be kept by the financial institutions for five years from the time the transactions were carried out, and the data used to verify the customer's identity must be kept for five years after the termination of the business relationship with the customer.

5

Additional measures for specific customers and activities

Recommendation 12 – Politically exposed persons (PEPs)

5.26. **Belgium is partially compliant with R 12** – Several deficiencies are observed: The definition of PEPs in the AML/CFT Law is limited insofar as only persons who exercise or have exercised important public functions and who live abroad can be considered PEPs. The criterion of residence abroad excludes, as such, foreign PEPs residing in Belgium and domestic PEPs or persons exercising or who have exercised an important function within or on behalf of an international organisation. Moreover, Belgian law provides a restrictive list of persons who are to be considered direct family members or close associates of PEPs, which is too restrictive compared with the open approach of R 12. The definition of PEPs also stipulates that, one year after PEPs have ceased their functions, they should no longer be considered PEPs. Finally, there are no specific provisions in Belgium requiring financial institutions to verify whether the beneficiary of a life insurance contract or its ultimate beneficiary is a PEP. These deficiencies can be attenuated in practice – however not in a systematic manner since it is based on an analysis of the risks under which financial institutions operate – by the general requirements to determine the risk profile of the customer and enhanced due diligence needed for higher risk situations. This series of gaps is considered to be a moderate shortcoming, given their scope with regard to the FATF requirements and their importance in an area calling for enhanced due diligence.

Recommendation 13 – Correspondent banking

5.27. **Belgium is partially compliant with R 13** – The law lays down the principle of applying enhanced due diligence measures for cross-border correspondent operations with financial institutions located in third countries considered as high risk, under the conditions provided for by R 13. Nevertheless and pursuant to Art. 12§4 of the law which applies 'without prejudice ... the exemptions referred to in Art.11 §1 1^o', the measures do not apply in relations with financial institutions originating in another EEA State or a third country that imposes control obligations equivalent to those set out in the 3rd AML/CFT Directive. Given the open and cross-border nature of the Belgian banking sector and the fact that the Recommendations consider cross-border correspondent banking as a high-risk activity, the deficiencies observed are moderate.

Recommendation 14 – Money or value transfer services

5.28. **Belgium is largely compliant with R 14** – The provision of money or value transfer services (MVTs) meets the conditions of R 14, including when they are provided through agents. However, there is no clear policy on the sanctions applicable to persons who provide MVTs without a license or registration, which would make it possible to judge whether such sanctions are proportional.

Recommendation 15 – New technologies

5.29. **Belgium is largely compliant with R 15** – Belgium has not developed a specific analysis of the ML/TF risks to which the financial system is exposed as a result of using new technologies. However, even though the law does not expressly provide for it, the general AML/CFT framework takes these risks into account to some extent, either by applying the enhanced due diligence rules applicable when contracts are concluded remotely, or by determining ‘specific risk criteria’ as grounds for the risk-based approach and the initial determination of the customer’s risk profile.

Recommendation 16 – Wire transfers

5

5.30. **Belgium is partially compliant with R 16** – Belgian law is based on EC Regulation 1781/2006, which does not contain all of the requirements in R 16. More specifically, it does stipulate any obligation to include information on the beneficiary of the wire transfer. Provisions on the obligations of intermediary financial institutions are also limited. The regulation is currently being revised to allow for these requirements to be included.

Reliance on third parties, controls and financial groups

Recommendation 17 – Reliance on third parties

5.31. **Belgium is partially compliant with R 17** – The conditions set out by R 17 for reliance on third parties to introduce business are not fulfilled with respect to the country in which these third parties are established. On the one hand, the exception set out in the RD of 19 July 2013 exempts the financial institution from ensuring that AML/CFT measures of a third country situated in an EEA State or in an equivalent third country are adequate. On the other hand, inclusion on the list of equivalent third countries takes into account risk-related information, without this analysis being targeted on ML/TF risks. These shortcomings are considered moderate, particularly in the Belgian context because the financial institutions are very open to European and international relations.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

5.32. **Belgium is partially compliant with R 18** – Financial institutions are required to implement AML/CFT programmes as set out in R 18, except for the requirements regarding the audit function for certain small entities (intermediaries in banking and insurance services, bureaux de change) and thus has a limited impact. The legislation imposes the development of a co-ordinated AML/CFT programme only for financial groups headed by a credit institution or an investment firm. Moreover, the actual content of the obligations to be implemented in this programme is not specified in the legislation or regulation, nor is the need for group subsidiaries and branches to follow AML/CFT rules compatible with the level required in the home country. This deficiency is considered to be moderate in the Belgian context which is characterised by a significant proportion of financial institutions that are part of financial groups, a number of them operating throughout Europe, and for which it would be important that AML/CFT programmes be co-ordinated and clarified at group level.

Recommendation 19 – Higher-risk countries

5.33. **Belgium is largely compliant with R 19** – Transactions with higher-risk countries are covered under the conditions required by R 19. However, Belgium does not have instruments allowing it to apply countermeasures to these countries independently of any call by the FATF to do so.

Reporting of suspicious transactions

Recommendation 20 – Reporting of suspicious transactions

5.34. **Belgium is compliant with R 20** – The AML/CFT Law provides that, when persons or institutions covered by the law know or suspect that a transaction to be carried out is related to ML or TF, they are to inform the CTIF. Criminal law covers the financial benefits (*avantages patrimoniaux*) of any criminal offence, whereas the AML/CFT Law covers a list of offences (covering all of the FATF designated categories of offences), but those covered do not have to determine which offence is concerned, so the difference between the two laws has no impact on those covered by the law.

Recommendation 21 – Tipping-off and confidentiality

5.35. **Belgium is compliant with R 21** – Financial institutions, their directors, officers and employees are protected by law from criminal and civil liability if they report their suspicions in good faith to the CTIF. The law also protects them from any threat, hostile act or intimidation. Additionally, the reports are not included in the files forwarded by the CTIF to the prosecutor's office or its foreign counterparts, in order to protect the anonymity of the source of the reports. Likewise, the persons or organisations that submitted a report cannot, under any circumstances, inform the customer concerned or any third parties that the information has been submitted to the CTIF.

5

Designated non-financial businesses and professions (DNFBPs)

Recommendation 22 – DNFBPs: customer due diligence

5.36. **Belgium is largely compliant with R 22** – Company service providers are not covered by Belgian AML/CFT measures. The CDD obligations set out in the AML/CFT Law, and the measures with regard to record keeping, PEPs, new technologies and reliance on third parties, apply to DNFBPs, who are accordingly affected by the limitations identified in R 10, R 12, R 15 and R 17. CDD requirements (R 10 rated LC) are central for R 22, but the shortcomings observed are only minor. Moreover, the failings with regard to reliance on third parties (R 17 rated PC) have less impact on the activities of DNFBPs.

Recommendation 23 – DNFBPs: Other measures

5.37. **Belgium is largely compliant with R 23** – The AML/CFT Law's measures on STRs, internal controls, higher-risk countries, and tipping-off/confidentiality apply to DNFBPs, with a number of adjustments for STRs and internal controls. DNFBPs are affected by the limitations identified in R 18, R 19 and R 20. More specifically, it should be noted that there is no independent audit function to check the AML/CFT system for any of the DNFBPs. It seems that, in this area, the characteristics of the DNFBPs must be taken into account, and in particular the small size of the entities to which these measures would have to be applied. The impact of this shortcoming is therefore limited.

5.3 Effectiveness: Immediate Outcome 4 (Preventive Measures)

(a) Understanding of AML/CFT risks and obligations

5.38. *Financial institutions* – **On the whole, a sound understanding was observed of ML/TF risks by the financial sector interviewed**, with regard to both activities (e.g. wealth management) or products (e.g. insurance products with a single premium, or associated tax benefits) and customers' characteristics (e.g. offshore companies, customer's geographic location/residence criterion) or business sectors (e.g. sectors that still make heavy use of cash, or the sectors dealing in diamonds, real estate, construction, and second-hand cars).

5.39. The new players in the financial sector (payment and electronic money institutions) demonstrated their understanding of the risks, especially those associated with cash refunds/withdrawals of electronic money, or the use of prepaid cards. Money remittance service providers also understood the risk of TF and the possibilities of being used for that purpose.

5.40. There was also a **sound understanding of ML/TF risks by the diamond banks** interviewed (which represent around 70% of the sector). **Bpost also has a sound understanding of ML/TF risks**, both for the financial services provided in its own name (electronic money, postal remittances and postal money orders) and for the money remittance service provided as agent of a market-leading EEA payment institution.

5.41. **The financial sector generally has a sound understanding of AML/CFT obligations**, except for certain bureaux de change, whose activities are at risk for ML/TF. Some confusion was noted, particularly concerning the notions of beneficial owners and PEPs, and the requirements pertaining to them in terms of determination/identification.

5.42. *DNFBPs* – **The understanding of ML/TF risks is patchy among DNFBPs**. Notaries, for example, have a sound understanding of the specific risks they have to address (company formations, real estate transactions, misuse of third-party accounts). Various sectors have identified the types of transactions or customers that represent a risk in their activities, which are described in the rules for applying the AML/CFT Law (e.g. notaries, real estate agents) or in circulars relating to these rules (accounting/tax professions, diamond merchants, secure cash transportation firms).

5.43. **Some sectors underestimate their exposure to ML/TF**. An example is **diamond traders**, whose sector-specific risk assessment by the industry trade group presents an unbalanced image of the sector (see Section 1). The same holds for **casinos**. Even though they are at risk because they handle cash and because of the growth of online gambling, they place their ML/TF risks in the broader perspective of the development of illegal casinos and the differences in neighbouring countries' legislations.

5.44. Certain sectors, including casinos, diamond traders, lawyers and accounting/tax professions, firmly believe that the regulations and supervision imposed on them are such that ML/TF risks are greatly reduced for those working in compliance with the rules of the profession. According to them, any risks would therefore be caused essentially by persons outside the regulated profession, or professionals violating their own rules. This is especially true for the actions involved in setting up and running companies. It is interesting to note though, that sector-specific risk analyses are in progress for lawyers and accounting/tax professions¹⁵, mainly in response to the national ML risk assessment, which identified vulnerabilities in their sector (see Section 1), in relation to which they have expressed reservations.

(b) Implementation of measures commensurate with the risks

5.45. *Financial institutions* - The assessment team met with a broad range of financial institutions and asked them very wide-ranging questions about all of the AML/CFT obligations. The replies were as expected from professionals in the matter: they gave the assessors insights into the implemented preventive measures, and highlighted the difficulties encountered through various examples. **Even so, the competent authorities should tighten AML/CFT controls to ensure that the obligations of all those covered by the system are properly applied** (see Section 6).¹⁶

5.46. **The financial sector institutions interviewed (banks and insurance companies) indicated they implement AML/CFT measures that are commensurate with and appropriate to the risks** (particularly regarding classification of customer risks). They implement these measures in two ways. The first is through their customer acceptance policy (based on criteria such as residence in Belgium or not, structure when the customer is a legal person, the expected value of the transactions, the declared or known business activity

15 The assessment for the accounting/tax profession was completed after the on-site visit.

16 This preliminary remark should also be taken into account for points (c) and (d).

or occupation, the country risk, etc.), updated on the basis of changes in the risks and the results of ongoing supervision of the transactions. The second way is by applying suitable due diligence.

5.47. Some of the payment institutions interviewed indicated that, when they are acting in their own name or as agent for a major EEA institution in the money remittance sector, they employ a policy of thresholds for managing transactions, based on the risks. These are thresholds above which the transaction is declined, or warning thresholds above which an additional due diligence is performed (predetermined amounts per transaction and over a number of transactions, with a reference code assigned to customers to monitor developments in their transactions).

5.48. Concerning country risk, the financial institutions indicated that they reassess the risk for certain countries on the list of equivalent third countries (RD of 19 July 2013) and do not automatically apply simplified measures, if they believe the country presents risks.

5.49. Nevertheless, **difficulties were observed in evaluating risk situations, and the proportionate, appropriate nature of the measures taken to effectively address them, particularly among certain bureaux de change.** For example, at a bureau de change acting in its own name, inadequate due diligence measures were noted in circumstances that clearly called for additional due diligence measures (e.g. accepting exchange transactions for large amounts with embassy employees, or with the embassy itself, with the only due diligence measure being to ask the embassy for a document certifying that it knew the source of the funds). The controls carried out by the FSMA detected the inadequacy of the measures taken and the case of the bureau de change in question was forwarded to the FSMA auditor in charge of examining the case in view of imposing an administrative fine, if relevant. The case is being investigated. Likewise, at a bureau de change acting as an agent for an EEA payment institution (and thus under the supervision of the BNB), the transaction monitoring thresholds applied consistently to all customers are inappropriate because they are too high for private individual customers (e.g. USD 4 500 per transaction).

5.50. *DNFBPs* – The assessors met with representatives of DNFBPs and, based on the interviews conducted and the documentation provided, observed the manner in which AML/CFT obligations were understood and applied, and the difficulties encountered. However, the competent authorities should tighten ML/TF controls to ensure that the obligations of all those covered by the system are properly applied (see Section 6).

5.51. **The basic AML/CFT obligations were generally understood by the DNFBPs interviewed, but applied mechanically without taking into account the potential risks** and with a view to meeting compliance objectives more than mitigating any ML/TF risks. A number of DNFBPs, including real estate agents, notaries, accounting/tax professions and casinos, operate with a repeat, local customer base whose habits and type of transactions are known. When an aspect of the intended transaction departs from this 'model', the professional adopts a more cautious approach and asks the (potential) customer more questions before proceeding with the transaction. It is only when they find themselves in the higher-risk situations described in their regulations, if applicable (notaries, real estate agents), that they will apply additional measures after having accepted the customer.

(c) Customer due diligence (CDD) measures and record keeping

5.52. *Financial institutions* – **Know-your-customer and ongoing due diligence measures form the foundation of the AML/CFT system for the financial sector.** This is true, for instance, for money remittance institutions (e.g. collecting information about the profession, questions about the connection with the beneficiary to prove the economic purpose of the transfer). A number of bureaux de change interviewed identify their customers (generally walk-in customers) whatever the value of the intended transaction, or starting at a threshold below that laid down by the legislation (EUR 10 000 - Art. 7 §1 2° of the AML/CFT Law).

5.53. The diamond banks indicated they sometimes had difficulty collecting know-your-customer information or information justifying certain transactions. In any case, they stated that they apply enhanced due diligence measures in this area, which they deem to be high-risk, and can eventually decline transactions or even, on rare occasions, break off or decline to enter into a business relationship.

5.54. **To carry out the determination/identification of beneficial owners**, the banking and insurance institutions interviewed apply a system based firstly, and sometimes primarily, on a signed statement by the customer or the customer's representative (e.g. the trustee of a legal arrangement), which is subsequently verified. In the event of difficulties, especially in situations with a foreign connection, these institutions indicated that they applied additional due diligence measures. If there is still doubt as to the determination/identification of the beneficial owner even after taking 'reasonable' steps (Art. 14, Regulation of 16 March 2010) (e.g. to understand the legal arrangements, in connection with taxation considerations), the institutions indicated that they submit an STR. Information from the supervisors as to what can be considered 'reasonable steps' in this area would give financial institutions guidance or practical solutions to help them more effectively conduct their search for beneficial owners.

5

5.55. The obligation to decline to enter into a business relationship or carry out a transaction once a business relationship has been established, for lack of sufficient information (knowledge of the purpose of the business relationship, the customer or the source of the funds involved in a transaction) or because identification cannot be established, seems to be met. An STR is generally submitted in these cases.

5.56. However, the obligation to break off the business relationship or not carry out a transaction during the business relationship, because of it is not possible to apply the required due diligence measures, more specifically to identify the beneficial owner, does not always appear to be met. The banking and insurance sector emphasised the commercial, technical and/or legal difficulties sometimes encountered in complying with this requirement. The question was raised, for example, in relation to the updating of beneficial owner identification data, which was the subject of a horizontal check by the BNB in 2012/2013. Life insurance companies mentioned legal considerations associated with insurance law that were difficult to reconcile with the obligation to terminate a business relationship (e.g. term insurance or life insurance tied to mortgage credits). To offset these difficulties, measures were taken to restrict the services available and prohibit any further transactions on the contracts in question (the contract was 'frozen', and it was impossible to pay the premium to the beneficiary at the end of the contract without proper identification of the beneficial owner).

5.57. The interviewed payment institutions that provide money remittance services decline transactions in the absence of identification and verification of the customer's identity, which is carried out in Belgium regardless of the amount. A European payment institution operating through agents in Belgium keeps and distributes to all of its agents a 'black list' of persons banned from business relationships and/or any further transactions, unless these persons provide the additional information required. This list is without prejudice to the implementation of asset-freezing screening obligations and the taking into account of FATF lists (see Section 4).

5.58. **Bpost indicated that it carried out identification and identity-verification due diligence measures for its own services** (postal remittances and postal money orders). It believed that there was a heightened risk of ML/TF because it was required to accept cash deposits and payments without any limit on the amount because of its public service mission. It also mentioned that there were situations in which it detected unusual transactions (a significant amount, an amount split into smaller amounts, etc.), which it would like to decline because of the risks. In that case, it submits an STR. **Bpost would like to be able to simply decline cash transactions in excess of EUR 3 000** (the threshold set by the AML/CFT Law, see above).

5.59. **No particular difficulty was noted in relation to** keeping records of transactions and of information obtained through due diligence measures.

5.60. *DNFBP* - **DNFBPs generally seem to comply with the customer identification requirement**, even if this requirement and the need to regularly update the information was hard to accept in sectors marked by long-standing business relationships and close ties with the customer (diamond traders and notaries in particular).

5.61. Because diamond merchants need to carry out their transactions quickly, identification is generally (in 70% of cases) limited to obtaining the customer's identity document - natural person, acting on behalf of a legal person if applicable - before the transaction, while the information received is verified and the documents concerning the legal person are obtained afterwards. This practice can be problematic, especially

as the diamond traders' customers are often from geographic zones considered to be high risk, in particular taking into account the origin of the rough diamonds, and it can be difficult to verify the information about them. This raises the question of whether (enhanced) due diligence measures can effectively be applied in these situations.

5.62. **There are also concerns about identifying online gamblers on authorised websites.** They are supposed to fill in an online form and attach a copy of an identity document. They are then assigned a unique 'player token', but there is no verification of their identity document. The Belgian Gaming Commission would like to be granted direct access to the National Register (of physical persons) (see R 10) for verification purposes, to prevent a customer from being assigned more than one *token* and also to apply the measures limiting the sums that can be played.

5.63. The area that represents the greatest difficulties for all non-financial stakeholders, especially in situations with foreign connections, is identifying the beneficial owner. Some professions use tools provided by specialised information service providers, but the great majority rely on the customers to forward the statements they made to the bank about their beneficial owners. Concerning the verifications required, it can be problematic that certain professions, such as diamond traders or real estate agents, stated that they systematically rely on the controls implemented by other stakeholders, respectively banks and notaries.

5.64. In general, the obligation to refuse to carry out a transaction if the due diligence obligations cannot be met seems to be sufficiently understood but seems to be applied only in cases of highly unusual transactions. In spite of everything, stakeholders only rarely consider submitting an STR. A number of DNFBPs reported the potential difficulties of continuing a business relationship with a customer for whom an STR was submitted.

5.65. **No particular difficulty was noted in relation to keeping records** of transactions and information obtained during due diligence measures.

(d) Enhanced due diligence measures

5.66. **Financial institutions - The financial sector, in general, implements enhanced due diligence measures in situations** recognised as high-risk situations by the FATF and the AML/CFT Law.

5.67. **The implementation of measures to detect/identify non-domestic PEPs can, in some cases, pose a problem.** Customers are generally invited first to sign a statement about whether or not they are a PEP. The institutions indicated that they refuse to enter into a business relationship if the prospective customer will not sign the statement. Further checks are carried as far as is reasonable (using search tools or lists drawn up by major outside service providers), but problems remain in some cases, such as false positives, difficulties regarding names or homonyms, and links with certain countries. The institutions regularly run checks for PEPs in their customer databases. Monitoring of the customer relationship with PEPs is adjusted to the risk (type of transactions, country, amounts, etc.). The institutions interviewed stated they were also already careful about domestic PEPs, and were anticipating the 4th AML/CFT Directive, specifically in situations that might present risks of influence peddling or national level corruption.

5.68. **For correspondent banking, enhanced due diligence measures are implemented on a risk-based approach**, with increased attention, for example, when the correspondent is located in an offshore centre or in certain countries where the supervision system is deemed less mature. When the financial institution is part of a group and the prospective correspondent is already in contact with the group, information about the institution may be exchanged within the group. Anti-corruption aspects are also examined. Less use is made of enhanced due diligence measures in the SEPA area,¹⁷ except for certain countries such as Switzerland. There are two main reasons for this. The first is the existence of the SEPA: a standardised means of payment

17 Single Euro Payments Area – There are 33 countries in the SEPA area: the 28 EU Member States plus Iceland, Liechtenstein, Norway, Switzerland and Monaco.

harmonises the processing of national and international orders,¹⁸ and the area can use the same payment systems and common BIC and IBAN identification codes. The second reason is the possibility of implementing simplified measures for relations with financial institutions in an equivalent third country (see R 13).

5.69. **Less use is made of enhanced due diligence measures on wire transfers within the EU** because the originator information required is simpler and there is no obligation to provide information on the beneficiary (Regulation 1781/2006, see R 16). In practice, full information on the originator is not always shown in the messages accompanying wire transfers when there is an intermediary institution between the originator's institution and the beneficiary's institution.¹⁹The same holds for information on the beneficiary. This can make it more difficult to implement certain due diligence measures. In SEPA formats, the name of the wire transfer's originator is required information. Information on the beneficiary of the wire transfer also exists,²⁰ but is not required information as described in Regulation 1781/2006 and does not include information on the beneficiary's name as described in R 16. In practice, this information is usually mentioned or requested by financial institutions, mainly so that it can be checked against OFAC and European lists. The banking sector representatives interviewed stated that, for domestic wire transfers, screening was carried out on the customer and the beneficiary. For intra-European transfers or transfers with third countries, asset-freezing screening is also carried out on the originator customer and on the beneficiary, within the limits of Regulation 1781/2006 for transfers within the EU, and on the financial flows. To identify persons who may be concerned by restrictive measures, the institutions interviewed implement screening measures using OFAC then EU lists; they also use commercial lists. This screening is carried out on entering into the business relationship and on receiving transaction requests. The institutions indicated there was good co-operation with the CTIF, the prosecutor's office and FPS Foreign Affairs in these matters concerning international sanctions for TF (see Section 4).

5.70. Outside the banking and insurance sector, it was not clear whether the financial sector representatives interviewed do indeed implement the enhanced due diligence measures required with regard to certain obligations, especially given their sometimes hazy understanding of the notions of beneficial owners and PEPs. For online banking activities, the financial institutions implement basic know-your-customer requirements and endeavour to establish a personalised contact with the customer, either by telephone or face-to-face. In particular, the procedures for verifying customers' identities are more difficult to carry out.

5.71. Examples of enhanced due diligence measures in cases other than those stipulated by the law were cited by the banking institutions interviewed. For example, in the case of anonymous donations to customers set up as religious associations (non-profit associations, ASBLs), a bailiff was asked to certify that the deposits did indeed correspond to the proceeds of the ASBL's fund-raising. The transaction was accordingly accepted under these conditions, with increased due diligence measures on these cash deposits, especially if they were followed by wire transfers.

5.72. **DNFBPs - No specific measures seem to be implemented by DNFBPs to detect PEPs.** They rely almost exclusively on the customer's statement on a form. Only certain professionals use PEP lists provided by specialised websites and if they do, they rely solely on the information contained in these lists. The

18 An additional transition period up to 1 August 2014 had been accepted, even though European wire transfers and direct debits came into general use on 1 February 2014, as per Reg.260/2012 (the 'SEPA Regulation').

19 Even if, in principle, an 'MT 202 COV' SWIFT message applies and gives the intermediary institutions full details of the originator.

20 Reg.260/2012 states 'where available, the payee's name' in relations between the payer and the payer's payment service provider (PSP) (Annex 2 a) iv); in relations between the payer's PSP and the payee's PSP, the payee's name is not required, but instead 'any payee identification code' and 'the name of any payee reference party' (Annex 2 b) vi) and vii) of Reg.260/2012).

EPIS²¹ database developed by the Belgian Gaming Commission, and used by casinos to check whether their customers are banned from gaming, does not contain information about this.

5.73. Regarding relationships with customers from countries considered high risk by the FATF, the majority of the professionals and businesses interviewed on site indicated they are familiar with the list, which is accessible through the CTIF website, and refer to it when they are dealing with a foreign (non-EU) customer. In that case, enhanced due diligence measures would be applied.

5.74. There is confusion in some sectors between this list of high-risk countries and the lists of persons and organisations subject to targeted financial sanctions, and also regarding the measures to adopt when dealing with customers from these countries or shown on these lists. Notaries, however, seem to have made a clear distinction between the two, and apply the necessary measures. The other sectors, because the customers they deal with are mostly national or even local, give only relative importance to these requirements.

(e) *Suspicious transaction reports (STRs)*

5.75. It is important to distinguish between 1) 'subjective' STRs based on suspicions of ML/TF, 2) 'objective' reporting based on criteria or thresholds fixed by legislative or regulatory provisions and submitted without any suspicion, and concerning mainly DNFBPs (e.g. Art.21 of the AML/CFT Law, RD of 1999 for casinos) and 3) 'automatic' reports that are not based on an ML/TF analysis or suspicion but are submitted systematically for a customer or type of transaction that has already been reported.

5.76. *Financial institutions - The financial sector has generally adopted the practice of suspicious transaction reports (STRs)*, even if diamond banks' reporting policy should be tightened, given the risks associated with this sector. In the bureau de change sector, it was noted that one establishment alone has been submitting over 97% of the sector's STRs over the last few years. A significant share of the STRs made by this bureau de change were automatic reports, based on the amounts involved, and these were not follow-up STRs, that is, additional STRs on a customer for whom one or more STRs had previously been submitted and which would be useful for continuing to follow the flow of transactions. This bureau de change was moreover one of the Belgian agents of a European payment institution, and similar practices on the part of other agents acting for this institution were also observed. This practice is similar to 'defensive' reporting, i.e. reports are submitted systematically for all further transactions carried out by a customer for whom a report had previously been submitted (for example, more than 70 STRs for the same customer). The large numbers of automatic STRs submitted can impair the effectiveness of the AML/CFT system. Awareness raising by FSMA and CTIF should be carried out jointly in order to inform the bureaux de change about the approach to take in repeat reporting on the same customer and the distinction between a follow-up report and an automatic one.

5.77. The banking and insurance sector interviewed spoke of difficulties in **detecting transactions that might be involved in laundering the proceeds of tax fraud**, and hence in the STRs to be submitted on the basis of such suspicions. The question of defining the new legal notion of 'serious tax fraud, organised or not', which was introduced by the Law of 15 July 2013, is said to contribute to legal uncertainty.²² For the Belgian authorities, though, financial institutions should submit an STR whenever there is suspicion of serious tax fraud. This question is currently the subject of an appeal before the Constitutional Court. Investigations by the police or the prosecutor's office were mentioned, along with BNB on-site inspections conducted at the request of these authorities to check for failures to submit a STR, or delayed STRs. Sanctions had been imposed in connection with this point (based on the regime preceding the Law of 15 July 2013, which nevertheless covered 'serious, organised tax fraud using complex mechanisms or procedures with an international dimension').

21 Created by the RD of 15 December 2004 (Ministry of Justice, 2005), EPIS (Excluded Persons Information System) is an information processing system containing the names of persons banned from gaming establishments. People on the EPIS list will not be allowed to enter these establishments.

22 Febelfin (2014b).

PREVENTIVE MEASURES

Table 5.2. Number of STRs submitted to the CTIF by financial institutions and DNFBPs

	2010	2011	2012	2013	% 2013
Bureaux de change and payment institutions (money remittance) ¹	11 491	12 364	11 716	11 657	50.76
Credit institutions	3 870	3 831	4 768	5 690	24.78
Casino operators	912	952	916	919	4.00
Bpost	471	634	800	1 085	4.72
Notaries	163	319	587	967	4.21
Accounting and tax professions ²	46	52	99	139	0.61
Life insurance companies	76	81	84	196	0.85
Statutory auditors	28	18	23	48	0.21
Real estate agents	26	28	22	67	0.29
Brokerage firms	25	23	20	22	0.10
Mortgage companies	42	37	17	12	0.05
Insurance intermediaries	18	13	10	18	0.08
Lawyers	0	1	10	9	0.04
Management companies for collective investment schemes	1	1	5	20	0.09
Bailiffs	3	5	4	8	0.03
Banking and investment service brokers	0	1	2	5	0.02
Diamond traders	1	6	1	1	-
Consumer credit companies	5	4	1	22	0.10
Finance leasing companies	0	1	1	0	-
Security companies	0	0	1	2	0.01
Payment institutions operating as credit card issuer and manager ³	0	4	7	6	0.03
Others ⁴	18	1	14	1	-

Source: CTIF

- 1 Since entry into force of RD of 2 June 2012 amending the list of organisations covered by the AML/CFT Law.
- 2 Outside chartered accountants, outside tax consultants, outside certified accountants, outside certified tax accountants.
- 3 Since the entry into force of the RD of 6 May 2010 amending the AML/CFT Law (Ministry of Justice and Ministry of Finance (2010)).
- 4 Clearing entities, investment management and investment advisory companies, branch offices of EEA financial institutions, collective investment funds, *Caisse des dépôts & consignations*, and market operators.

5.78. The institutions interviewed did not mention any problems in relation to the non-disclosure and confidentiality requirements concerning STRs.

5.79. *DNFBPs* – **The commitment to suspicious transaction reporting varies widely from one DNFBP to another.** The practice of STRs grounded on subjective criteria has been taken on by notaries and, to a certain extent, by the accounting/tax professions, even if the number of reports, which has risen steeply in recent years, tends to remain limited. This upturn in the quantity and quality of reports can be attributed to the awareness-raising initiatives conducted in these sectors. **The number of STRs submitted by casinos seems extremely high, but corresponds to automatic reports** based on objective indicators contained in the RD of 1999 (e.g. when a customer purchases chips to the value of EUR 10 000 or higher and pays in cash or using a bank or credit card; note that this threshold is checked only when the chips are exchanged at the end, not as the gaming operations are carried out, and that this can undermine the effectiveness of the measure). It seems that real estate agents also rely almost exclusively on objective factors to submit a report (cash payments are prohibited for real estate transactions under Art. 20 of the AML/CFT Law).

5.80. For other professions identified as particularly vulnerable to ML/TF, such as **lawyers and diamond traders, virtually no reports are submitted to the CTIF.** In the case of lawyers, STRs have to first go through the filter of the president of the bar (*bâtonnier*), who does not check the substance (the ‘appropriateness’ or *opportunité* of the report) but verifies that the criteria required by the AML/CFT Law are met. Lawyers are subject to AML/CFT measures only for a limited series of operations, most of which have to do with real estate and financial transactions, and administering companies (Art. 3 5° AML/CFT Law). Their interpretation of the activities that should be reported as suspicious further narrows the scope of the obligation in that the suspected ‘criminal source of the money’ is not always linked to ML/TF, so does not prompt an STR. It seems that notaries share the same interpretation. Additionally, lawyers tend to have a broad interpretation of ‘the assessment of their client’s legal position’ (Art. 26 §3 2° of the AML/CFT Law), which would seem to exempt them from making a STR for information received from their client in this context.²³ A question arises as to the grounds for filtering reports through the president of the bar, a measure introduced when the system was established, to ensure that reports effectively lay within the scope of the law. Today it would appear that the conditions required by the law have been clarified and that lawyers are familiar with them. Allowing lawyers to report directly to the CTIF could help make STRs more transparent and provide better visibility into the suspicious transactions with which lawyers are confronted, for the CTIF and the profession as a whole.

5.81. Diamond traders also show great reluctance to report suspicious transactions, as can be seen by the small number of STRs and the amounts involved, which seem excessively small compared with the volumes handled by the profession. This attitude can be attributed to cultural factors, more specifically the tradition of discretion that unites diamond traders. The diamond traders indicated that they rely on their banks to decide whether or not to make reports.

(f) Internal controls

5.82. *Financial institutions* – **Internal controls and procedures designed to ensure compliance with AML/CFT obligations are in place in the financial sector.** There are first and second-level controls, including for Bpost (which operates on the same model and with the same compliance officer as Bpost Banque) and diamond banks. The latter indicated that internal audit is a key component of their preventive system, considered during discussions with the BNB. This organisation of internal controls is not necessarily as structured in small establishments, such as small bureaux de change (principle of proportionality).

23 Art. 4.72 last para. of the Code of professional conduct of the Order of the French-speaking Bar and the German-speaking Bar states that ‘When a lawyer dissuades his/her client from carrying out a transaction that could prompt a suspicious transaction report, the lawyer should not submit a suspicious transaction report to his/her president of the bar’ (Moniteur Belge / Belgisch Staatsblad, 2013).

5.83. *DNFBPs* – Internal controls and procedures designed to ensure compliance with AML/CFT obligations are in place in non-financial professions' larger organisations. Because of the small size of most non-financial stakeholders, this observation does not call for particular attention.

(g) Limitation on cash payments

5.84. **The limitations on cash payments** (10% of the total price of goods or services up to EUR 3 000, Art. 21 of the AML/CFT Law) **raise interpretation issues that have an impact on their application in practice.** They are intended to apply only to the sale by a merchant or a service provider, with the exception of precious metal purchases. However, both the seller and the buyer commit an offence and both can be prosecuted. The current wording and the competent authorities' interpretation of it do not however clearly delimit the scope of application. This impairs the legal certainty of the transactions carried out by certain merchants and control of cash movements. Moreover, clarification is needed concerning the way in which the measures in the AML/CFT Law connect with and are applied in conjunction with the other provisions applicable in this area,²⁴ and specifically the ban on cash purchases of copper and the measures applicable to precious metals.

5

5.85. **In conclusion**, financial institutions seem to have a good understanding of the risks. Not all *DNFBPs* appear to have grasped the full extent of the ML/TF risks to which they are exposed, nor the need to protect themselves against potential ML/TF misuse.

5.86. Financial institutions generally have a sound understanding of AML/CFT obligations, and the AML/CFT measures implemented are generally commensurate with and appropriate to the risks. There are, however, shortcomings for certain payment institutions and certain bureaux de change, particularly in their understanding of the requirements regarding beneficial owners and PEPs. The financial sector also seems to apply enhanced due diligence measures in recognised high-risk situations, though to a lesser extent for correspondent banking relationships and wire transfers within the EU.

5.87. Efforts have been made in recent years by a large number of *DNFBPs* to engage professionals and raise their awareness of AML/CFT concerns. These initiatives should be continued to ensure satisfactory implementation of the measures. The enhanced measures applied by *DNFBPs*, for example, seem limited for situations that require sustained attention. When *DNFBPs* are unable to meet CDD requirements, they say that they refuse the business relationship or the transaction, even if they do not send in a STR. The implementation of AML/CFT measures by diamond traders does not seem to be of a sufficient level to ensure that the sector's high risks are addressed.

5.88. The financial sector has, on the whole, adopted the practice of STRs. Even so, bureaux de change and certain payment institutions operating through a network of agents also carry out a significant proportion of automatic STRs, which do not provide additional information on the transactions of a customer that has already been reported. *DNFBPs* that are under obligation to report on the basis of thresholds/criteria often limit themselves to this type of 'objective' reporting and do not try to report on the basis of an assessment of whether or not a particular transaction is suspicious. There are still virtually no STRs from lawyers and diamond traders. Tighter AML/CFT controls by the competent authorities are necessary to ensure that *DNFBPs* adequately fulfil their obligations.

5.89. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 4.**

24 For example, the law of 29 December 2010, amended in July 2013, prohibits cash purchases of copper, and places sellers of old or precious metals under an obligation to identify customers who pay cash for amounts over EUR 500 (Chancellerie du Premier Ministre, 2010).

5.4 Recommendations on Preventive Measures

The AML/CFT legal framework

- Belgium should adapt its legislation to the 2012 FATF Recommendations, in particular with regard to reinforcing the risk-based approach, situations for which simplified due diligence measures may be applied, PEPs, correspondent banking, higher-risk countries, wire transfers, and new technologies.
- Belgium should clarify and simplify the legislation on cash payment limitations, concerning both its scope and the interaction with the various applicable measures.

ML/TF risks

- Belgium should ensure that supervisors and the persons and institutions covered by the law take into account the findings of the national ML and TF risk assessments in the risk analyses they develop at sector level, and at individual institution level, when appropriate. The persons and institutions covered by the law should also help update the national analyses, based on the risk situations encountered.
- Belgium should encourage the circulation of information on risk (sector assessments, typologies, thematic studies, inspection reports, etc.) between the public authorities (CTIF, BNB, FSMA, Police, etc.) and the private sector.

Understanding of and information on AML/CFT

- The supervisors and industry trade groups of DNFBBs should take initiatives to promote and explain the applicable AML/CFT rules, to increase the effectiveness of their implementation.
- Supervisors should put into place targeted, tailored educational initiatives, based on the guidelines, for certain financial institutions (bureaux de change, payment institutions, electronic money institutions) and the DNFBBs, concerning the notions of beneficial ownership and PEP.
- Belgium should increase consultation and dialogue with the private sector to explain AML/CFT obligations when necessary and clarify what is expected of those persons and institutions covered by the law (e.g. guidelines, reviews of initiatives by the FIU and the supervisors).

Implementation of the risk-based approach

- The Belgian authorities should guide and support the DNFBBs in their process of assessing ML/TF risks at sector level.
- Belgium should support the determination of priorities by the various non-financial sectors, to address these risks and to put proportionate preventive measures into place.

Suspicious transaction reports (STRs)

- Belgium should revise the procedure for STRs to be submitted by lawyers and its merits in the light of the experience gained.
- For diamond traders, Belgium should pursue awareness-raising and educational initiatives on reporting obligations. Suitable initiatives, likely to bring about a change in professionals' motivation and involvement, should also be organised with the industry trade group.
- For casinos, Belgium should revise and update the RD of 1999, which sets out the transactions that should be reported to the CTIF.

PREVENTIVE MEASURES



Bibliography

- Assuralia (2014), *Canaux de distribution de l'assurance – Chiffres 2012*, Assuralia, Brussels, www.assuralia.be/fileadmin/content/stats/02_Overige_AssuraliaStudies/Distributiekanalen/FR_Distribution_2012.pdf (French only).
- BNB (2013), *BNB Annual Report 2013, Statistical Annex*, BNB, Brussels, www.nbb.be/doc/ts/Publications/NBBReport/2013/EN/T2/report2013_T2_annex.pdf
- Chancellerie du Premier Ministre (2010), *Loi portant des dispositions diverses, 29 décembre 2010* Chancellerie du Premier Ministre, Brussels, www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2010122901&table_name=loi (French only)
- Eurostat (2013), *Transfers by migrants to their country of origin remained stable at nearly 39 bn euro in 2012*, Eurostat News Release, 187/2013 - 10 December 2013, <http://ec.europa.eu/eurostat/documents/2995521/5168122/2-10122013-AP-EN.PDF/3c235475-1e11-4071-9435-6e6f7f241664?version=1.0>
- FATF (2005), *Mutual Evaluation of Belgium*, FATF, Paris, www.fatf-gafi.org/countries/a-c/belgium/documents/mutualevaluationofbelgium.html
- FATF (2013), *Money laundering and terrorist financing through trade in diamonds*, FATF, Paris, www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-through-trade-in-diamonds.html
- Febelfin (2014a), *Chiffres-clés 2012-2013 (Facts & Figures, 2012-2013)*, Febelfin, Brussels, www.febelfin.be/sites/default/files/files/ff_fr_2014_gmr.pdf (French only)
- Febelfin (2014b), *Le secteur financier demande plus de clarté et de sécurité juridiques dans la lutte contre la fraude fiscale grave*, press release, January 2014, Febelfin, Brussels, www.febelfin.be/fr/le-secteur-financier-demande-plus-de-clarte-et-de-securite-juridiques-dans-la-lutte-contre-la-fraude
- FSMA (2014), *FSMA Annual Report 2013*, FSMA, Brussels, www.fsma.be/~media/Files/fsmafiles/pub/en/fsma_2013.ashx
- Gaming Commission (2013), *The Belgian Gaming Commission's official list of A+ licences attributed to casinos in Belgium*, 2013, Gaming Commission, Brussels, www.gamingcommission.be/opencms/export/sites/default/jhkweb_nl/documents/Ax.pdf
- Ministry of Justice (2005), *Arrêté royal relatif à la création d'un système de traitement des informations concernant les joueurs exclus des salles de jeux de hasard de classe I et de classe II*, Royal Decree, Brussels, www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2004121532&table_name=loi (French only)
- Ministry of Justice and Ministry of Finance (2010), *Arrêté royal portant adaptation de la liste des organismes soumis à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme*, Royal Decree, Brussels, www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2010050602 (French only)
- Ministry of Justice, Ministry of Finance et al (2011), *Arrêté royal mettant en oeuvre l'évolution des structures de contrôle du secteur financier*, Royal Decree, Brussels, www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2011030301&table_name=loi (French only)
- Moniteur Belge / Belgisch Staatsblad (2002), *Loi relative à la surveillance du secteur financier et aux services*

PREVENTIVE MEASURES

financiers, 6 August 2002,
www.fsma.be/~media/Files/fsmafiles/wetgeving/wet_loi/2002-08-02_Wet-Loi.ashx

Moniteur Belge / Belgisch Staatsblad (2013), *Publication conforme aux articles 472 à 478 de la loi-programme du 24 décembre 2002, modifiés par les articles 4 à 8 de la loi portant des dispositions diverses du 20 juillet 2005*, 17 janvier 2013, Brussels,
www.ejustice.just.fgov.be/mopdf/2013/01/17_1.pdf (French only)

World Bank (2013), *Remittance Prices Worldwide*, World Bank, Washington,
<http://remittanceprices.worldbank.org/en/countrycorridors>

5

6. SUPERVISION

Key Findings

Financial institutions

In the financial sector, the supervisors have generally identified the main high risks. Understanding of the risks is not, however, sufficiently ongoing, due to the insufficiency of the controls carried out, and especially on-site inspections.

To date, there is little implementation of controls by the BNB based on ML/TF risk. There are few on-site AML/CFT inspections, and this can be explained by an inadequate assessment of the ML/TF risks to which the institutions are exposed and a shortage of resources. The BNB recently launched a periodic questionnaire to obtain specific, systematic information about ML/TF risks and more effectively prioritise supervision.

For the FSMA, the AML/CFT controls introduced address the bureaux de change sector, which was identified as the most at risk of ML/TF, and these controls are appropriate. Nevertheless, these controls should be strengthened so as to address the quality of STRs due to the large proportion of automatic reports. For collective investment fund management companies, investment management and investment advisory companies and mortgage providers, given the more limited risk associated with those activities, AML/CFT controls are included in the general on-site inspections. For the financial intermediary sector, there are no specific, qualitative on-site inspections to ensure compliance with AML/CFT obligations.

FPS Finance conducted on-site visits at Bpost, for information purposes, on the AML/CFT systems and procedures in place, but at this stage no measure/inspection as such has been conducted.

For the financial sectors under FPS Economy's supervision, no desk audit or on-site inspection has been conducted. However these are low-risk sectors (consumer credit companies, finance leasing companies).

The main financial sector supervisors follow a policy of fostering understanding of ML/TF risks and explaining AML/CFT obligations, essentially through a concrete, detailed guideline, joint BNB/FSMA circulars, and by referring stakeholders to the CTIF website and annual report.

DNFBPs

Efforts have been made in recent years to engage DNFBPs and raise their awareness of AML/CFT concerns. Supervisors have been designated and regulatory systems are in place. Certain professions (e.g. notaries and the accounting/tax professions) have become very actively involved in promoting AML/CFT measures. This role is played mainly by the industry trade groups, such as for diamond traders or real estate agents, with the support of the supervisor.

DNFBP supervisors have generally identified the greatest risks. However the systems to monitor developments in these risks and ensure that they are known and understood have yet to be set up.

In general, the controls of the DNFBDs are still very limited, if not non-existent. The risk-based approach, when it exists, is confined to the assessment contained in the annual AML/CFT report, which determines the businesses to be inspected as a matter of priority, while the inspections subsequently carried out are standardised.

In a number of non-financial sectors, such as legal and accounting/tax professions, assigning responsibility for controls to working professionals could be detrimental to the effectiveness of the supervision.

For financial and non-financial sectors alike, the limited controls and the significant lack of sanctions taken solely on ML/TF matters have a major impact on the effectiveness of AML/CFT measures.

6.1 Background and Context

6.1. *Financial institutions* – In 2010, **the overall structure of Belgian supervision of financial institutions**, organised around the Belgian Banking, Finance and Insurance Commission (CBFA), **was re-engineered**¹. The supervision model introduced rests on two pillars (the ‘Twin Peaks’ model):

- a prudential pillar, assigned to the National Bank of Belgium (BNB), which exercises the various prudential supervision functions in relation to credit institutions, investment companies with the status of brokerage firm, insurance and reinsurance companies, clearing and settlement services, payment institutions, electronic money institutions and mutual guarantee companies;
- a supervisor, the Financial Services and Markets Authority (FSMA), which, on one hand, exercises all of the supervision functions over stakeholders not subject to prudential supervision and financial markets and products, and, on the other hand, supervises the rules of conduct of stakeholders in the financial sector and supervises consumer information and protection. It is responsible for collective investment funds, collective investment fund management companies, investment companies with the status of investment management and investment advisory companies, bureaux de change, market operators, insurance and reinsurance intermediaries, banking and investment service intermediaries, and businesses and operations related to mortgage credit.

6.2. Supervision of the financial institutions under the responsibility of the BNB and the FSMA also covers compliance with AML/CFT obligations. Co-operation between the BNB and the FSMA is governed by a Protocol signed in March 2013. It allows them to exchange information so that they can co-ordinate their supervision policies, including in AML/CFT matters, and ensure that their interpretation of the system is identical and that they are implementing consistent supervision measures and procedures. This co-ordination is especially important in AML/CFT matters in cases where the spheres of responsibility are shared. For example, where investment companies are concerned, the FSMA supervises investment management and investment advisory companies, while the BNB supervises brokerage firms. In insurance, the BNB is responsible for insurance companies, while the FSMA supervises the intermediaries.² The table shown in Section 5, point 5.1.(b) presents the authorities responsible for the various financial institutions.

6.3. With the introduction of the Single Supervisory Mechanism for banks in November 2014, the European Central Bank (ECB) became the sole authority competent for the direct prudential supervision of significant European banks³ and will accordingly **exercise direct supervision over Belgian financial groups**.⁴ However, the **supervision roles not assigned to the ECB - one of which is to prevent the financial system from being used for ML/TF purposes - will remain the responsibility of the national**

1 The reform was described in Communication CBFA_2011_15 du 23 mars 2011 (CBFA, 2011)

2 It should also be noted that the BNB and the FSMA share competence for supervision of the Euroclear group: the BNB supervises securities settlement systems and the group’s banking operations, while the FSMA supervises the protection of investments and the rules of conduct in relation to the financial markets.

3 More specifically, banks with assets worth in excess of EUR 30 billion or representing at least 20% of their home country’s GDP, or which applied for or received direct financial support from the European Financial Stability Facility or the European Stability Mechanism, or which have substantial cross-border operations (Art. 6.4 Reg. 1024/2013, Official Journal of the European Union, 2013). For cross-border banks, the existing procedures for co-ordinating supervisors from the home country and the host country will continue to apply. For institutions where the ECB will take on the role of direct supervisor, it will fulfil the functions of home country authority and host country authority for all of the participating Member States.

4 Banque Central Européenne (2014).

authorities.⁵ The other banks remain under the exclusive prudential supervision of the national authorities - the BNB, as it happens - but the results of this supervision will be reported to the ECB.

6.4. Under the **rules governing the European passport**, EEA financial institutions operating in Belgium through a branch office (under freedom of establishment) are subject to AML/CFT supervision by the Belgian authorities, in co-operation with the authorities in their home country. EEA financial institutions operating in Belgium without being established there (under the freedom to provide services) are subject to AML/CFT supervision by the authorities in their home country. Payment and electronic money institutions from another EEA Member State who offer payment services in Belgium through agents based in Belgium (a form of freedom of establishment) are subject to the AML/CFT Law. They should designate a person to be responsible for compliance with the Belgian AML/CFT law, who must be located in Belgium. AML/CFT supervision of the establishment by the Belgian authorities will be carried out through this person, the 'central point of contact'.

6.5. **FPS Finance is responsible for supervising Bpost** with respect to financial activities for which it is covered by the AML/CFT regime (see Section 5). Bpost also acts as an agent for a major European payment institution's money transfer operations in Belgium. Within this framework, FPS Finance is also competent to supervise this European payment institution operating through Bpost, for which it is also the central point of contact (see Section 5 and c. 14.3).

6.6. **FPS Economy is responsible for supervising finance leasing companies and consumer credit institutions.** It is also responsible for supervising compliance with the limitations on cash payments (see Section 3).

6.7. **DNFBPs - The Law of 18 January 2010** added a new Art.39 to the AML/CFT Law, which **transfers responsibility for the AML/CFT supervision of DNFBPs from the CTIF to the supervisors, supervisory government authorities or disciplinary authorities of these businesses and professions.** The table shown in Section 5, point 5.1.(b) shows the authorities responsible for AML/CFT supervision of the various DNFBPs.

6.2 Technical Compliance (R 26 – R 28, R 34, R 35)

Recommendation 26 – Regulation and supervision of financial institutions

6.8. **Belgium is partially compliant with R 26** – For the financial institutions subject to their supervision, the BNB and the FSMA have set up processes and tools to define their prudential risk profile, of which ML/TF is one of the components, but without the BNB's having identified the amount of ML/TF risk for each of the institutions. With the exception of the bureaux de change supervised by the FSMA, the extent and frequency of ML/TF controls are not stipulated specifically on the basis of the type and level of ML/TF risk identified for each of the institutions. The BNB and the FSMA regularly review the risk profile of the institutions under their supervision, though there is no indication what role ML/TF risk plays in the scope of this review. FPS Finance, which is in charge of supervising a major European payment institution for the money remittance service provided in Belgium through Bpost, does not specify the supervision method applied. This is also true for FPS Economy, although it is in charge of lower-risk sectors (consumer credit companies and finance leasing companies).

Recommendation 27 – Powers of supervisors

6.9. **Belgium is largely compliant with R 27** – The BNB and the FSMA have the general powers to supervise, oversee and sanction financial institutions, including by applying the enforceable means at their

5 'The ECB should co-operate, as appropriate, fully with the national authorities which are competent to ensure a high level of consumer protection and the fight against money laundering.' Official Journal of the European Union (2013).

disposal within the broader framework of their powers to impose sanctions in prudential matters. FPS Economy and FPS Finance, on the other hand, have only the sanctions provided for by the AML/CFT Law, which are confined to information measures and administrative sanctions.

Recommendation 28 – Regulation and supervision of DNFBPs

6.10. **Belgium is partially compliant with R 28** – There are a number of shortcomings: the absence of requirements for fit and proper checks in the diamond trade sector, which is recognised as high risk. Furthermore as a general rule, supervision programmes, when they exist, were drawn up without any individualised assessment of professionals’ risk, nor reference to the sector’s risk. What impact the stakeholders’ risk profile has on the extent and frequency of controls is not indicated.

Recommendation 34 – Guidance and feedback

6.11. **Belgium is largely compliant with R 34** – The competent authorities, and more specifically the CTIF, in addition to a number of supervisors and self-regulatory bodies, circulate information of a general or thematic nature on AML/CFT matters and draw up guidelines for the persons and institutions covered by the law. It is to be noted, however, that no specific measures have been taken recently by FPS Finance or FPS Economy, or by the authorities in charge of security companies, casinos, lawyers registered with the French- or German-speaking Bars, or bailiffs. The CTIF circulates general feedback in the annual report, which presents relevant statistics for each sector, along with typologies based on an analysis of the reports. The supervisors do not take part in or take the initiative in providing sectorial feedback in relation to the implementation of reporting obligations, on the basis of observations made during their inspections. Such actions might help reporters detect and report suspicious transactions.

Recommendation 35 – Sanctions

6.12. **Belgium is largely compliant with R 35** – A diverse range of criminal, administrative and disciplinary sanctions are available to prudential supervisors, and can be applied, either specifically or through prudential controls, for failure to fulfil AML/CFT obligations. However, to gauge the proportionality of the sanctions, there is no indication of whether and how the scale or nature of these sanctions might vary with the nature and extent of the non-compliance observed, the institution responsible for the non-compliance, the seriousness and number of violations, whether or not it was a repeat offence, or other relevant criteria. When sanctions are imposed on legal persons, their directors and officers may also be sanctioned. For certain DNFBPs, this involves imposing a disciplinary sanction against the director.

6.3 Effectiveness: Immediate Outcome 3 (Supervision)

(a) Approvals and ‘fit and proper’ checks on directors and shareholders

6.13. *Financial institutions* - The BNB has mechanisms for verifying that directors and significant or controlling shareholders are *fit and proper*, both when applications have been submitted for licencing or registration, and when the BNB receives mandatory notice of changes of directors or shareholders. These procedures are set out in BNB circulars that the assessment team was able to consult. These verifications mainly consist in checking the criminal record or requests to the prosecutor’s office for information on any legal proceedings in progress. The BNB records instances in which it was in contact with the judicial authorities for criminal cases involving prospective directors, which might call into question their suitability for directing a financial institution. These checks may also rely on the international co-operation of foreign counterparts when the situation involves cross-border elements. The BNB indicated that it is extremely rare that it formally refuses an approval on ‘fit and proper’ grounds, because approval applications that are problematic on these points are systematically withdrawn by the applicants concerned when they are examined by BNB staff. The BNB told the assessors about several cases in which, when it had requested further information on the capacity of the shareholders, the applications had been withdrawn or the plans cancelled, for example concerning the sale/purchase of an insurance company. The BNB also cited an example in which it had refused a banking

license because the status of the majority shareholder, a transnational finance company, may have made it difficult to carry out effective consolidated supervision.

6.14. **The FSMA also has supervision mechanisms in place to verify the capacity of the directors and shareholders who exercise control over the companies** under its responsibility. It uses them when applications have been submitted for licensing or registration, and when the FSMA receives mandatory notice of changes of directors or shareholders. It cited the case of requests to change the shareholder structure, which were turned down because of the difficulty in tracing the source of the funds to be used to purchase the securities. It can also use foreign counterparts, though this does not happen often, given the essentially domestic character of the institutions under its control. The FSMA also has a department dedicated to identifying cases of illegal practice of financial activities, which refers around 20 cases per year to the public prosecutor's office.

6.15. **DNFBPs – The business practices of DNFBPs are subject to conditions designed to avert the risks of infiltration by criminals or their accomplices.** As a general rule, applicants for registration or licensing are required to supply a certificate of good character, which provides information about any convictions in the applicant's police record. Only diamond traders are not subject to fitness and properness conditions, but FPS Economy may use its discretion to refuse registration. For lawyers and statutory auditors, registration and supervision of the professional register fall, respectively, to the public prosecutor's office and the Prosecutor General.

6.16. Despite this supervision, an isolated case still in progress was noted in which the supervisor of statutory auditors had not withdrawn the professional qualification of a person who had been convicted on appeal of forgery and use of forged documents, forgery and use of forged tax documents, fraud and tax fraud in the exercise of his professional functions, which may raise reservations on the effectiveness of supervision in this area.

6.17. The Belgian Gaming Commission considers that the greatest ML/TF risk facing casinos is that of being infiltrated by criminals. Accordingly it performs very thorough checks on the establishments' potential shareholders and directors before granting a licence (face-to-face interviews, application of subjective criteria to assess the capacity of the shareholders, etc.), and may communicate with other government agencies, in particular the tax authorities. The Commission has also drawn up a *black list of illegal gaming websites* in Belgium, which do not have access to a server in Belgium.

6.18. As a general rule, **information is required on DNFBPs' shareholders, including changes that occur over the course of the business's existence, and violations of this requirement are subject to sanctions.** For the accounting/tax and legal professions, the majority of shares and voting rights within associations and groups must be held by certified professionals. The certification authorities/supervisors ask the managers to provide a statement about the beneficial owners and/or the register of shareholders. For real estate agents and diamond traders, there are no requirements about providing information on the shareholders. However, FPS Economy is currently taking steps to obtain directly from registered diamond traders the identity of shareholders who hold over 25% of the shares in their companies.

6.19. There is cause for concern in the fact that legal and tax advisory services are available from persons who are not members of regulated professions and are not subject to any AML/CFT obligations, or from professionals who violate the rules governing their practice, including in ML/TF matters. This is particularly true for company formation and carrying out the various legal acts pertaining to the life of companies. Besides the fact that these activities may be deliberately misleading about the capacity of the person who performs them, they may also result in operations aimed at misusing companies for the purposes of ML/TF. The lack of regulations for domiciliary companies (see Section 5) heightens the risks of these mechanisms misusing legal persons. This issue also raises the question of the effectiveness of the controls applied to certain DNFBPs.

6.20. The real estate agents' industry trade body conducts ongoing, effective action to prosecute individuals practising the profession without a licence.

*(b) AML/CFT controls of financial institutions***Controls by the BNB**

6.21. *Understanding of ML/TF risks - As a general rule, the BNB has identified the main financial activities under its supervision exposed to ML risks:* money remittance services, and in particular those involving a network of agents, activities associated with cash movements, wealth management, with concerns regarding knowledge of the source of the funds (in the recent, specific context of the *Déclaration Libératoire Unique* tax amnesty, which gave Belgian taxpayers an opportunity to regularise their tax position⁶), or electronic money and online banking, which nevertheless appear to be relatively limited in their use at this point. Bank customers' business sectors are also risk factors, in particular certain businesses in which transactions are mainly carried out in cash, such as second-hand vehicle sales or cleaning companies.

6.22. **The BNB stays informed of the emergence and evolution of ML/TF risks through outside sources** that cover primary ML/TF phenomena (information in the college of supervisors, European fora such as the European Commission or the European Supervisory Authorities, FATF, the press, etc.). It focuses on supervising the procedures and systems set up by the financial institutions to detect unusual transactions and effectively address threats. It does not, therefore, take a proactive approach to gain insights into the criminality associated with ML/TF, and acts in response to warnings or confirmed instances of ML/TF, which it believes the CTIF or the professional sector are responsible for identifying and monitoring. However, as part of its controls and its information initiatives, an authority can also be in a position to identify ML/TF phenomena that would not otherwise have been identified, and help to identify ML/TF risks and ensure that the financial sector understands them and that they are addressed by AML/CFT prevention systems. This step would give the BNB input to the risk-based approach that it is going to pursue and strengthen for carrying out its AML/CFT controls (see below). The BNB should also ensure that outside information on the risks, which are many and diverse, is fed into this effort so that the BNB operational departments in charge of organising compliance controls can access and consult it. The BNB should also analyse any data it holds that might be relevant for AML/CFT (e.g. information about wire transfers collected under Target 2).

6.23. **The BNB indicated that it will include the relevant risks shown in the national ML and TF risk assessments** in the risk-based approach it is going to pursue and strengthen for carrying out its AML/CFT compliance controls. It has nevertheless conducted specific initiatives on the sectors identified as high-risk sectors by the national ML risk assessment. For example, in 2010 and again in 2013, the BNB drew financial institutions' attention to the risks associated with large cash movements (deposits or withdrawals), especially in connection with gold transactions.⁷ It also mentioned an example of an investigation it had conducted into a *systemic* bank that had made a delayed STR to the CTIF regarding large cash withdrawals. The BNB took action after being informed by the prosecutor's office, which had been informed by the CTIF. This example underscores the need for the BNB to regularly co-operate with the CTIF (see Section 1), especially as credit institutions are among the main reporters to the CTIF (see Section 5), and to permit it in this way to actively contribute to the ML risk assessment.

6.24. Concerning TF risks in the financial sector, the main focus of attention is the money remittance sector. For the rest, and especially where wire transfers are concerned, the BNB underscores the need for the rule-based application of asset-freezing obligations.

6.25. *Helping stakeholders understand AML/CFT risks and obligations - Policy on building stakeholder understanding of ML/TF risks and AML/CFT obligations relies essentially, to date, on a concrete,*

6 Law of 11 July 2013 amending the tax regularisation regime and establishing a social regularisation.

7 BNB/FSMA (2013).

detailed⁸ **guideline**, joint BNB/FSMA⁹ circulars issued in response to warnings from the CTIF or confirmed instances of ML/TF, and advice to consult the CTIF website and annual report. Moreover, the BNB's annual report contains very little information about its AML/CFT policy.

6.26. **The BNB should be encouraged to take a more proactive approach**, based on a review of its supervision operations and leading to initiatives to educate and inform stakeholders. Joint initiatives with the CTIF should be organised, in particular with regard to STRs. The financial sector interviewed unanimously called for regular feedback on STRs so that it could ultimately obtain a sector-specific overview of the reports made, similar to what currently exists, informally, with the major banks' compliance officers. The financial sector appreciates and uses the tools already provided by the CTIF, and in particular its annual reports, which contain useful statistics and typologies. A more direct, targeted and frequent dialogue with the CTIF and the BNB, based on on-site inspections of the institutions' reporting policy, would give each sector a qualitative appraisal of the reports received and guidance for raising the quality of the reports. It would also help change the approach of certain payment institutions that provide money remittance services either directly or through a network of agents, and which submit a large percentage of automatic STRs. It would also be desirable to **co-operate more closely with the CTIF on typologies** affecting the financial sector. Initiatives to take advance measures, as was done for freezing mechanisms with regard to Ukraine, would make it possible to include these cases in financial institutions' warning and monitoring systems (e.g. the use of illegal Brazilian labour in the industrial cleaning sector, the construction sector, or used car sales/purchases involving West Africa).

6.27. *ML/TF risk-based controls* - **The BNB examines prudential risk at sector level and for each institution.** Accordingly, institutions are classified into *systemic, core, current, small* and *industrial supervision*. Within each of these categories, the risks to which each institution is exposed are periodically assessed on an individualised basis to determine the appropriate supervision actions ('scorecarding').¹⁰ This overall risk assessment includes an assessment of ML/TF risks, as a sub-criterion of the 'compliance' criterion. However, there does **not appear to be a clear, specific definition and organisation (type and level) of ML/TF risk analysis for each sector and each institution**. So, while there is an individual prudential rating, it has neither been established nor derived from a specific assessment of the institutions' AML/CFT risk even if this aspect has an influence on the overall rating. For the insurance sector, there is however a map of AML/CFT risks for each product, which could not be replicated for the other sectors and for which, according to the BNB, the product/business approach would not be as useful.

6.28. **When on-site inspections or specific off-site controls are conducted, the ML/TF risk-based approach is not yet sufficiently organised.** The understanding of each institution's individual risks is based on the knowledge derived from overall prudential supervision, examination of the annual AML/CFT report, and the annual interviews, which will determine which institutions are to be inspected. The BNB is nevertheless making an effort to expand the information on which it bases its assessment of ML/TF risks: it recently brought in a periodic AML/CFT questionnaire.¹¹ This tool was developed in consultation with the profession. It is currently undergoing improvements and should give the BNB a systematic, ongoing understanding of ML/TF risks.

6.29. However, **the complementarity and hence the effectiveness of the supervision/reporting tools (the AML/CFT report and the periodic questionnaire) are still in question**, mainly because of the BNB's

8 CBFA (2010).

9 For example, BNB/FSM (2013).

10 The risk assessment carried out in *scorecarding* is structured into three main areas: 1) Environment, which includes governance, environment, general profile, solvency and financial ratios; 2) horizontal functions, which includes audit, risk management, compliance - including the AML/CFT aspect - management control, IT, outsourcing, business continuity plan-business recovery plan; 3) risks, which includes credit, interest rate, market, cash assets, operations, asset management.

11 BNB (2013).

shortage of resources for processing and monitoring them. The questionnaire is welcome for smaller entities of the banking and insurance sector and new entrants in the financial sector (such as payment institutions or electronic money institutions).

6.30. To date, the risk-based approach (based essentially on prudential risks) applied by the BNB has led it to concentrate its on-site inspections on larger institutions. On the other hand, we noted a serious insufficiency if not an almost total lack of on-site AML/CFT inspections of small and medium-sized banks (classified as *current* or *small*). Inspections of so-called *systemic* institutions are warranted, including for AML/CFT purposes, but they should not make up the bulk of on-site inspections for the banking and insurance sector. The supervision approach should include a definition of a minimum frequency for inspections of smaller-scale 'baseline' institutions.

Table 6.1. Inspections

Type of inspection – Credit institutions and investment companies	Number from 01/01/2010 to 01/07/2014
Total prudential inspections	150
of which inspections including one or more AML/CFT-related components	47
of which inspections focused <u>exclusively</u> on AML/CFT	7
Total recommendations made during AML/CFT inspections	207
AML/CFT inspections: coverage of the banks and brokerage firms sector (criterion used: balance sheet total)	73.56% ¹
Type of inspection – Insurance companies	Number from 01/01/2010 to 01/07/2014
Total prudential inspections	45
of which "internal control systems"	16
of which inspections focused <u>exclusively</u> on AML/CFT	2

Source: BNB

1. This figure does not include second or third AML/CFT inspections of the same institution during the specified period.

6.31. **The serious insufficiency of on-site AML/CFT inspections lessens the effectiveness of the AML/CFT prevention system** and makes it impossible to be certain that the financial institutions are meeting and properly implementing the requisite obligations. **It also impedes ongoing understanding of the risks. The lack of on-site inspections or follow-up action since the interviews conducted with the diamond banks following the publication in the press of the 'Monstre Worldwilde'¹² affair illustrates the difficulty of achieving continuity in risk assessment.**

6.32. The low number of inspections is also due to an **acute shortage of resources, and the BNB needs to significantly increase its available resources**. More specifically, this will be necessary for it to be able to carry out the ambitious programme of on-site inspections scheduled for 2014 at eight payment and electronic money institutions. These new non-bank stakeholders were licensed only recently, so should be allowed to

12 An international courier company organised illegal diamond movements for 355 diamond merchant customers, enabling them to evade paying tax on these transactions. The investigation into this affair began in 2004 and the fraud is estimated at nearly EUR 800 million.

operate for a sufficient period of time before an on-site inspection¹³ is held, to enable an in-depth review. But in July 2014, only one on-site inspection was in progress on the first payment institution licensed in 2010.

6.33. **No on-site inspections have been conducted to date at the 17 EEA payment institutions operating in Belgium through a network of agents** (nearly 1 500 agents), even though **money remittance services, especially those provided through a network of agents, are considered a high-risk business in Belgium and throughout the EU**. One of these European service providers - a major industry player - has the largest network of agents in Belgium. One of these agents is Bpost, which has a culture and an understanding of AML/CFT. The gaps in the European framework concerning the determination of the competent authority for supervising these institutions have not allowed the BNB to take decisive action as the competent authority of the institutions' host country. Belgium recently brought in various measures to remedy these shortcomings, and now has a complete map of the *central points of contact* (CPCs) appointed by European payment institutions. The CPC is the supervisor's contact person in the host country: the supervisor's questions/requests to the payment institution covered by the system go through the CPC. The CPC also comes under supervision, by virtue of a right to require information, because the services are provided through these agents (see TC Annex, C.14.3). It should be noted that the European payment institution that provides money transfer services in Belgium through Bpost and another network of agents has two CPCs: one is supervised by the BNB, the other by FPS Finance (through Bpost). Each of these supervisors accordingly supervises the European payment institution that does business with the network of agents for which it is competent. The BNB and FPS Finance should co-ordinate their efforts to ensure that their controls are carried out using equivalent methods.

6.34. The BNB has just launched a **periodic AML/CFT questionnaire**, modelled on the questionnaire applied to institutions licensed in Belgium, for European institutions established in Belgium solely in the form of networks of agents or distributors. It lays the groundwork for off-site supervision of these institutions. It is a simplified version of the questionnaire, adjusted to suit institutions operating in Belgium through a very small number of agents, or which run a very limited number of operations there.

6.35. Nearly **270 European payment institutions operate in Belgium under the freedom to provide services**, mainly to offer money remittance services. They come many from the United Kingdom (188 institutions were noted). Under European law, AML/CFT compliance supervision falls to the competent authority in the home country. The BNB explained that money remittance activities carried out under freedom to provide services in Belgium consist in transactions that go through an account held by a Belgian institution, which reduces the risk of ML/TF associated with these transactions.¹⁴ For their compliance controls, Belgium relies on the supervision of the competent authority of the country of origin and the quality of the due diligence carried out by the Belgian institution under its supervisory authority. The prevention of ML/TF activity by this channel depends therefore on the quality of supervision of these institutions. No information was provided on the cross-border co-operation with the competent authorities in question. There were also no information on any safeguards put into place by the Belgian authorities to ensure that European payment institutions comply with the principles of the freedom to provide services, for which supervisor from the country of origin is competent.

6.36. The on-site AML/CFT inspections conducted by the BNB, which are very limited, **do not appear to be based on an in-depth or thematic approach** that would provide closer and more effective supervision. For instance, it is not clear that certain aspects or activities that present or might present high ML/TF risks (e.g. diamond banks, cash deposits/withdrawals – outside the gold sector – third-party accounts) are analysed or monitored to any significant extent within the framework of these on-site inspections.

13 Moreover, some statutory auditors have already submitted installation reports to check that all of the procedures described are effectively in place.

14 However, the money remittance transactions which are exposed to a higher risk of ML/TF take place through the acceptance of cash payments to an agent or teller located in Belgium, and operating under the freedom of establishment.

6.37. The Single Supervisory Mechanism for banks (see point 6.1) was not in force at the date of the on-site inspection (it took effect on 1 November 2014), so was not taken into account for the assessment. The BNB should nevertheless define the resources to be allocated, in particular for co-ordination with the ECB, and adjust its overall risk assessment system described above. It should also consider possible changes in the prudential risk analysis and classification system in place, which includes AML/CFT.

6.38. *Remedial action and sanctions* – Only two cases related to ML/TF have been opened to date. **The lengthy processing and follow-up on the findings in on-site inspection reports** – in particular for the referral to and examination by the auditor, and the possible subsequent referral to the BNB sanctions committee – **weaken the only two cases** related to ML/TF, currently pending, given the defendant's right to a reasonable timeframe. Here again, the lack of resources is one of the causes.¹⁵ In any case, the significantly insufficient number of on-site inspections and the lack of a specific AML/CFT risk-based approach in the action priorities are the main factors behind the insufficient number of cases submitted for sanctions.

6.39. Insufficient remedial measures, including administrative sanctions,¹⁶ and the complete lack of disciplinary sanctions in AML/CFT matters in recent years also impair the effectiveness of AML/CFT efforts. They are the direct outcome of a serious insufficiency of AML/CFT controls, and in particular on-site inspections.

6

FSMA controls

6.40. *Understanding of ML/TF risks* – **The FSMA has identified the main ML/TF risks presented by the institutions under its responsibility and has developed matrices** that measure these risks in terms of likelihood of occurrence and impact for the sector. The operations most at risk are those of bureaux de change, because of the cash movements involved in these transactions. However, the small sums involved in these transactions and the small number of institutions (12) limit the impact of these risks. Additionally, because there are so few bureaux de change, the FSMA knows them well. The FSMA breaks down bureaux de change by risk level (*high, medium, low*), which determines the extent and frequency of the control measures implemented.

6.41. **The risks associated with the operations of collective investment fund management companies and investment management companies are considered moderate**, since these businesses cannot receive customer assets, and the assets are simply managed or advice given, not moved from one institution or account to another. **Regarding financial intermediaries**, given the size and the characteristics of the sector, the risks seem limited in terms of both instances of ML/TF and their impact (see Section 5).

6.42. With the exception of supervision of the bureaux de change sector, the **understanding of the risks is neither ongoing nor exhaustive, given the insufficiency of AML/CFT controls** and in particular on-site inspections. It is based essentially on outside information sources and annual AML/CFT reports, except in the case of financial intermediaries, which are not required to produce AML/CFT reports.

6.43. *Helping stakeholders understand AML/CFT risks and obligations* - **Policy on building stakeholder understanding of ML/TF risks and AML/CFT obligations relies essentially, to date, on a concrete, detailed guideline, joint BNB/FSMA circulars issued in response to warnings from the CTIF or confirmed**

15 In the two cases in question, following the reform of the supervisory architecture in 2011, a new sanctions committee had to be set up, and the member appointment procedure was marked by very protracted delays and timeframes.

16 The BNB indicated that 14 serious administrative measures were taken against banks and brokerage firms between 1 January 2010 and 31 October 2013, but they all concern a horizontal (one-off) action conducted on the identification of beneficial owners, and the sanctions taken are laid down not in the AML/CFT Law but in banking law.

instances of ML/TF, and advice to consult the CTIF website and annual report.¹⁷ The FSMA does run some initiatives to educate and inform stakeholders, but they are limited (e.g. circular to remind life-insurance intermediaries of their AML/CFT obligations¹⁸). The only substantial information on AML/CFT controls in the FSMA annual report concerns bureaux de change.

6.44. **The FSMA should be encouraged to take a more proactive approach**, based on a review of its supervision operations and leading to initiatives to educate and inform stakeholders. Joint initiatives with the CTIF should be organised, in particular with regard to STRs, using the same approach as was recommended for the BNB (see above).

6.45. It is also important to check that employees involved in AML/CFT controls have adequate AML/CFT training, especially on the notion of beneficial owner and the steps to take when the beneficial owner is not identified, for which some bureaux de change have difficulties.

6.46. *ML/TF risk-based controls* – **Because of the high ML/TF risks in bureaux de change's operations, specific, in-depth AML/CFT controls are conducted, including document-based checks and on-site inspections.** The resources allocated seem appropriate (one full-time equivalent to carry out on-site inspections and off-site controls), given the number of stakeholders. They could be increased for greater effectiveness of the controls (for example concerning the quality of the STRs) and to cater to the requirements of the next on-site inspection programme, since the FSMA says that the 12 bureaux de change should be inspected on site every year. The observations made during on-site inspections concern the computer system and its ability to record and manage all of the identification data and other know-your-customer information, accurate data entry into the computer system by counter staff, or failure to carry out due diligence measures. **Some bureaux de change have also been found to have difficulty effectively detecting, analysing and reporting suspicious transactions to the CTIF.** One money changer in particular submits a large proportion of automatic STRs, which are not supplemental STRs relating to reports already made concerning a particular customer. This practice could lessen the effectiveness of the AML/CFT system (see Section 5). The fact that this practice has been going on for a number of years and is the work of one of the largest players in the sector, placed in the AML/CFT 'high risk' category in the FSMA classification, **raises questions about the level of supervision for STRs applied to this bureau de change. The FSMA's compliance controls for STR obligations by bureaux de change, and more particularly with this bureau de change should be tightened.** At the very least, steps should be taken to provide guidance to ensure that the CTIF reporting obligations are properly and effectively applied (e.g. during an inspection, review the controls carried out in the sector on this subject).

6.47. **The other sectors under FSMA responsibility** (investment management and investment advisory companies, financial intermediaries, collective investment fund management companies, mortgage credit services) **have a lower ML/TF risk profile.** Accordingly, the **controls on these services concern aspects other than AML/CFT**, and the implementation of AML/CFT risk-based controls consists, to date, in an appraisal of the annual AML/CFT report (except in the case of intermediaries). Following its examination, the FSMA may ask for changes to be made to the report. In 2012, 12 investment management and investment advisory companies and four collective investment fund management companies were asked to amend their reports, i.e. roughly 25% of the total. However, it is difficult to assess the effectiveness of the follow-up on this report for want of specific, qualitative AML/CFT on-site inspections.

6.48. Concerning intermediaries, because of their large number and the low degree of risk, except for off-site control of the licensing application, **there are no AML/CFT tools for off-site supervision of the sector**, nor are there tools that are adjusted and proportionate to the size and diversity of these entities. **On-site controls are based solely on indicators** (e.g. press articles, information from judicial authorities,

17 CBFA circular of 6 April 2010 and, for example, BNB/FSMA circular on recent changes concerning the prevention of money laundering (BNB/FSMA, 2013) (in French only).

18 FSMA (2013).

information provided by an insurance company, formal complaint). In the other cases, the FSMA indicated that it carried out AML/CFT awareness-raising instead during its general inspections.

Table 6.2. Number of Inspections with an AML/CFT Component

	2011	2012	2013
Insurance intermediaries	44 ¹	26	22 (of which 9 were at the main offices) ²
Banking and investment services intermediaries			0

Source: FSMA

1. A more specific breakdown for 2011 and 2012 is not available.
2. This number also includes inspections that were carried out at the main offices that were themselves responsible for verifying whether the intermediary met the necessary conditions for registration. The number of intermediaries concerned by these inspections is thus greater than the number of inspections carried out.

6.49. Based on information provided by FSMA on-site inspectors, **in practice, on-site inspections of the entities subject to inspection** (except bureaux de change, see above) **are general and not specifically directed towards** compliance with AML/CFT obligations. On-site inspections nevertheless include an AML/CFT component concerning collective investment fund management companies, investment management and investment advisory companies and mortgage credit services (e.g. whether there is an AML/CFT officer, whether there are AML/CFT procedures), the extent of which depends on the business concerned.

Table 6.3. Number of Inspections with an AML/CFT Component

	2012	2013	2014
Collective investment fund management companies	2	0	1
Investment management and investment advisory companies	0	7	0

Source: FSMA

6.50. The sectors referred to above were analysed as 'limited risk' of ML/TF by the FSMA, and it was therefore understandable that there were no on-site inspections dedicated exclusively to AML/CFT. **However, an increase in the number of AML/CFT inspections is necessary to ensure compliance with the obligations. With respect to intermediaries, an assessment of low risk should not lead to on-site checks that are limited as to compliance with AML/CFT obligations**, for example, whether AML/CFT measures and procedures are in place.

6.51. The FSMA indicated as well that it is currently reorganising its on-site inspection methods and re-allocating resources (it is setting up a 10-strong team of inspectors for financial intermediaries), **primarily to include AML/CFT concerns** in a general on-site inspection programme for the financial intermediaries sector.

6.52. *Remedial action and sanctions – An administrative sanction was taken in 2010* (by the CBFA) against a bureau de change, based on a non-compliance case opened in 2005. The bureau de change was required to pay a EUR 25 000 fine, and the authorities published the judgement (without naming the bureau de change) indicating the failure to discharge the obligations associated with unusual transactions, shortcomings in the performance of the function of AML/CFT officer, and failure to report suspicious transactions. **Another case is in progress, which also involves a bureau de change.** The AML/CFT inspection reports always indicate the remedial action to be taken.

Controls by FPS Finance and FPS Economy

6.53. **FPS Economy has a sound understanding of the risks related to finance leasing operations.** Regulatory measures are being finalised (estimated entry into force in 2015) to allow AML/CFT measures and controls to be implemented.¹⁹

6.54. **From the interviews with FPS Finance, which is in charge of Bpost, it appears that it is beginning to come to grips with the activities and risks concerning Bpost.** The reports on the recent on-site visits confirmed that the contacts were aimed at informing Bpost and establishing a sound understanding of the system, procedures and supervision tools used for AML/CFT. **No on-site inspection had been conducted** and no recommendations or points for improvement had been issued regarding Bpost. Regarding supervision of Bpost in its capacity as agent (and central point of contact) for a major European payment institution that offers money transfer services in Belgium through counter post offices, **no mention was made during the interviews of the actions taken or planned by FPS Finance to co-ordinate its control methods with the BNB**, which is responsible for supervising the other central point of contact designated for the second network of agents used by this payment institution in Belgium. As a general rule, co-operation and support initiatives on the part of the BNB in particular (which controls Bpost Bank) should continue so that FPS Finance can implement effective controls of Bpost's operations, in particular on-site inspections.

6

(c) *AML/CFT controls of DNFBPs*

6.55. *Understanding of AML/CFT risks and promotion of AML/CFT obligations* – In recent years, **many non-financial sectors have developed initiatives to engage professionals and raise their awareness of AML/CFT.** Supervisors have been designated and regulatory systems are in place. Certain professions (e.g. notaries) have become very actively involved in promoting AML/CFT measures. This role is played essentially by the industry trade groups (diamond traders and real estate agents, for example), with support from the supervisor. Training courses have been provided, along with learning and practical tools for professionals.

6.56. **DNFBP supervisors have generally identified the highest ML/TF risks, but they have not developed risk assessments** or guidelines for understanding the risks. Nor are there any systems to help them, or professionals, monitor developments in these risks and ensure that they are known, understood and taken into account when applying preventive measures and controls. Given these circumstances, it is important to point out the initiative taken by FPS Economy, in collaboration with real estate agents, to develop a computer application that should be operational by end-2015: it will make it easier to identify high-risk and unusual transactions, and will give FPS Economy a map of the agents the most at risk, to help with organising controls.

6.57. **With regard more specifically to STRs**, and with a view to raising their quality, joint initiatives should be organised between the DNFBP supervisors and the CTIF, using an approach similar to that recommended for the financial sector (see above).

6.58. *ML/TF risk-based controls* – **For many DNFBPs, steps have yet to be taken to check compliance with AML/CFT and risk-management obligations.** In any case, the resources assigned to this supervision seem insufficient as a general rule. This is especially true for FPS Economy, which is responsible for not only diamond traders and real estate agents but also finance leasing companies (and in a related field, controls of the limitations on cash payments). There are not enough inspectors for the number of entities to be inspected (eight employees in the central office and a pool of 100 regional inspectors for all of the areas under FPS Economy's responsibility), and inspectors are insufficiently trained in AML/CFT aspects. A greater focus on the risk-based approach, which FPS Economy has been actively working on, should make it possible to offset, albeit partially, these deficiencies.

¹⁹ Supervision of the consumer credit sector currently falls to FPS Economy, but no measures to apply AML/CFT rules and no supervision measures have been taken.

Table 6.4. AML/CFT controls carried out by DNFBPs

DNFBP	Supervisors	Inspection reports
Notaries	National Chamber of Notaries and Chamber of each of the 11 provincial companies	2012: 129 offices were inspected; 2013: 393; 2014 (including the controls programmed through the end of the year): 1173 Information on the results of these controls is not available
Statutory auditors	Institute of Statutory Auditors (IRE)	AML/CFT controls as part of quality control: 250 performed in 2014; 57 prompted follow-up on points related to AML/CFT obligations
Chartered accountants and tax consultants	Institute of Chartered Accountants and Tax Consultants (IEC)	AML/CFT questionnaire sent end-2012: 99.5% response rate. On-site inspections only if a disciplinary investigation has been opened AML/CFT checks as part of quality control: 36 professionals controlled in June/July 2014
	Professional Institute of Certified Accountants and Tax Accountants (IPCF)	Questionnaires sent out to all members in 2013. No on-site inspections as yet 3 disciplinary sanctions were imposed by the 2 institutes in the 1st half of 2014 including for failure to comply with AML/CFT obligations
Lawyers	Order of the French-speaking Bars and the German-speaking Bar and each of the 14 bars Order of the Flemish Bars and each of the 14 bars	French and German-speaking Bars: no inspections carried out Flemish Bar: 4 detailed reports on the application of preventive measures; no control as yet
Casinos	Belgian Gaming Commission (FPS Justice)	2013/2014: 14 inspections (full controls and not targeting AML/CFT exclusively) No AML/CFT compliance shortcomings observed and no sanctions imposed
Diamond traders	FPS Economy	2 inspections carried out in 2013/14, based on an analysis of annual AML reports 1 violation in relation to the limit on cash payments
Real estate agents (and chartered surveyors)	FPS Economy	4 inspections carried out in the 1st half of 2014 (then 6, one of which resulted in a warning and 3 requests for STRs).
Security companies	FPS Interior	Regulation was adopted in March 2014. No inspection had taken place since then
Bailiffs	Belgian National Chamber of Court Bailiffs	No information about the inspections carried out. First inspections scheduled for 2016

Source: Information from the Belgian Authorities

6.59. **The lack of AML/CFT controls contributes to the lack of follow-up and analysis of the risks.** In this respect, the purpose and goal of the AML/CFT controls conducted by the competent authorities sometimes remain to be clarified: many professions seem to use these controls to detect cases of ML/TF,

rather than to check whether AML/CFT preventive measures are being properly applied. There is also a significant difference between the way certain authorities describe the intensity of the controls and the way it is perceived by the entities controlled. Casinos, for instance, do not mention AML/CFT aspects among the aspects checked by the Belgian Gaming Commission.

6.60. **For some professions, the application of AML/CFT measures is checked as part of a broader quality control** on services or accounting (e.g. accounting/tax professions, casinos and notaries, except in one province). **But in other sectors, such as lawyers, such controls do not exist and are in the process of being introduced.** It should be noted that, legally, controls on third-party accounts, which are quite exposed to ML/TF risk, should be carried out by the president of the bar. For lawyers on the Dutch-speaking bar, controls should be conducted each year on at least 2.5% of the francs managed by the lawyers of each bar.

6.61. Questions should be asked about the extent of the responsibilities assigned to the professional bodies that play a key role in conducting AML/CFT controls (given that the disciplinary sanctions are in the hands of bodies made up of members from outside the profession), particularly as concerns the legal and accounting/tax professions. The lack of geographical proximity between the controllers and the controlled parties, or the involvement of honorary members of the profession in carrying out the controls, do not always appear to be sufficient to guarantee neutral, transparent controls. Moreover, with no distinction between the controllers and the controlled, the assessment of the sector risks cannot take advantage of the differing perspectives on ML/TF risks and vulnerabilities that the professions and the supervisors might bring. The involvement of third parties from outside the profession could bring a critical and objective view on the level and types of ML/TF risk and would thus be desirable.

6.62. The responses to a self-assessment questionnaire on compliance with AML/CFT obligations, or the annual AML/CFT report (when it is required by the regulatory provisions for applying AML/CFT law), will generally serve as the starting point for controls, when such exist, and determine which professionals should be controlled as a matter of priority, thereby factoring in ML/TF risks to a certain extent. In other cases, supervision is organised on a regular basis (every 3 years for notaries, for example, or for the quality control of statutory auditors of public-interest bodies, and every 6 years for other statutory auditors), without taking the risks into consideration.

6.63. **On-site inspections**, when they exist, last no more than a half-day or one day, and **focus exclusively on the main obligations laid down by law and formal compliance with them** (in particular, customer identification, record-keeping, and appointment of an AML/CFT compliance officer). The obligations concerning identification of the beneficial owner and PEPs and relations with high-risk countries and asset freezing do not seem to be covered by specific, appropriate controls. Suspicious transaction reporting does not seem to be examined either, nor does the inspector look at the quality of the reports submitted consider whether some of its transactions should have been reported. The selection of cases for testing may take the risk factor into account: for example, cases concerning a pre-nuptial contract at a notary's office will not be checked for AML/CFT aspects. It would also be necessary to ensure inspections look at whether asset freezing measures are in place and effective for all DNFBPs (see Section 4.4a).

6.64. *Remedial action and sanctions - Sanctions were imposed for AML/CFT matters in certain sectors, almost exclusively for failure to send in the annual AML/CFT report.* FPS Economy imposed EUR 1 000 administrative fines on 36 diamond traders on these grounds, and these measures prompted an increase in the number of annual reports sent to the supervisor. The disciplinary bodies of the IEC and the IPCF (accounting/tax professions) also imposed disciplinary sanctions for this non-compliance.

6.65. The IEC recently initiated quality controls that include an AML/CFT thematic component. In 2014, 36 controls were conducted (2013 are scheduled for 2015), but the shortcomings observed in four cases have, for the time being, only led to a follow-up control, which has to take place within six months. Statutory auditors imposed about 10 disciplinary sanctions between 2010 and 2013, mainly for non-compliance with AML/CFT regulations. In April 2013, following a question from the College of Prosecutors-General, the IRE reminded its members that, in the event of the dismissal of a statutory auditor for disciplinary reasons and signs of ML, the institute's board would refer the matter to the disciplinary bodies and tell them that they can impose an administrative fine. This reminder of the possibility of imposing administrative sanctions should

be circulated more widely. When controls reveal non-compliance with AML/CFT obligations, the level and frequency of the sanctions pronounced remain limited.

(d) Specific controls on cash payment limitations

6.66. **FPS Economy selects the sectors to be controlled on the basis of an analysis that takes into consideration risk and opportunity criteria**, based on complaints or information from outside departments such as the police or FPS Finance.²⁰ **Widespread controls have been conducted** over the last three years in the sectors of new and used vehicles, or gold, for example. They detected sums illegally paid in cash amounting to over EUR 1.1 billion. In 2011/13, 478 offences were observed and 32 cases referred directly to the public prosecutor's office as a serious offence. Over the same period, 446 administrative transactions were proposed, to the value of EUR 956 553. The fines imposed range from EUR 250 to EUR 225 000, capped at 10% of the sums unduly paid in cash (Art. 41 § 1 of the AML/CFT Law).²¹ While these sanctions may seem dissuasive in theory, it should be noted that, in 2013, fines totalling EUR 335 000 were imposed for 151 violations: this represents EUR 2 000 per violation, which seems a minor amount.

6.67. **FPS Economy does not yet have sufficient objective distance to be able to make an overall assessment of the impact of the controls.** Some sectors will be controlled again in coming years. There does appear to be a positive impact however on auction houses, which were the subject of an industry-wide investigation launched in 2013. After the control, auction houses changed their terms and conditions to clearly state that they no longer accept cash payments for amounts in excess of the legal limit.

6.68. The controls have certain limitations, though, more specifically because they are based solely on the accounts of the merchants and services providers, so cannot take into account any transactions that were not entered into the books. The resources allocated to these controls also remain limited.²² It seems moreover that, even if the various stakeholders interviewed indicated that they had noticed changes in the use of cash, this is still the usual means of payment for certain businesses.

6.69. **In conclusion**, in the financial sector, the supervisors have generally identified the main high risks. Understanding of the risks is not, however, sufficiently ongoing, due to the insufficiency of the controls carried out, and especially concerning on-site inspections. To date, BNB controls are conducted primarily using a prudential approach, and little use is made of AML/TF risk-based controls. There are few on-site inspections, due to an inadequate assessment of the ML/TF risks to which the institutions are exposed, and a shortage of resources. Shortcomings in supervision are particularly worrying in the case of financial institutions doing business in Belgium based on the European passport, under freedom of establishment, through agents in Belgium. The BNB recently launched a periodic questionnaire to obtain specific, systematic information about ML/TF risks and more effectively prioritise supervision.

6.70. For the FSMA, the AML/CFT controls introduced address the bureaux de change sector, which is identified as the most at risk of ML/TF, and are appropriate. Nevertheless these controls should be reinforced with regard to the quality of STRs given the large proportion of automatic reports. For the collective investment fund management companies, investment management and investment advisory companies and mortgage credit services, given the more limited risks associated with these activities, AML/CFT controls are included in more general controls. For the financial intermediary sector, there are no specific, qualitative on-site inspections to ensure compliance with AML/CFT obligations. A reinforcement of these controls is therefore necessary.

20 Some data is more difficult to obtain, such as customs data.

21 Further percentage increases have to be added to these fines - a system that increases the fine laid down by law by applying a legal coefficient, which is regularly adjusted to the current value of the money. The coefficient was X6 in February 2014, which brings the maximum fine to EUR 1 350 000.

22 See below for the resources available to FPS Economy.

6.71. FPS Finance made on-site visits to Bpost for information purposes, on the AML/CFT systems and procedures in place, but at this stage no on-site inspection has been conducted. For the financial sectors under FPS Economy's supervision, no inspections have been conducted. However these are low-risk sectors (consumer credit companies, finance leasing companies).

6.72. The main financial sector supervisors follow a policy of fostering understanding of ML/TF risks and explaining AML/CFT obligations, essentially through a concrete, detailed guideline, joint BNB/FSMA circulars, and by referring stakeholders to the CTIF website and annual report.

6.73. The DNFBP supervisors have been designated and the regulatory provisions are in place. The supervisors have generally identified the highest risks. However the systems to monitor the evolution of these risks and ensure that they are known and understood have yet to be set up. In general, supervision of the DNFbps is still very limited, if not non-existent. The risk-based approach, when it exists, is confined to the assessment contained in the annual AML/CFT report, which determines the businesses to be supervised as a matter of priority, while the controls subsequently carried out are standardised.

6.74. For the financial and non-financial sectors, closer co-operation should be organised between the supervisors and the CTIF, mainly to improve the policy applied by all reporting institutions, in particular concerning the quality of STRs. Moreover, the limited controls and the significant lack of sanctions taken solely on ML/TF matters have a major impact on the effectiveness of AML/CFT measures.

6.75. FPS Economy conducts targeted controls of compliance with the limitations on cash payments, and the ML/TF risk is one of the factors taken into account to select the sectors covered. It is difficult to gauge the results because the controls began only recently, but they have already brought about changes in certain professionals' practices. The resources allocated to these controls need to be increased to ensure that large-scale initiatives can be undertaken.

6.76. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 3.**

6.4 Recommendations on supervision

Implementation of ML/TF risk-based controls

- Analyses of sector-specific risks should be conducted, to identify the high-priority areas that require special due diligence measures on the part of the private sector and targeted controls by the competent authorities.
- The BNB should significantly increase the resources for ongoing control and on-site inspections, and the staff available to examine the cases requiring sanctions. It should step up ML/TF risk-based supervision and adjust its extent, frequency and intensity to the risks. The BNB should also carry out sufficient on-site AML/CFT inspections to address the risks.
- The authorities responsible for the AML/CFT controls of DNFbps should organise risk-based supervision covering all AML/CFT obligations. They should also increase the resources allocated to controls, taking into account the type and level of ML/TF risks in the various sectors. Belgium should ensure that the professionals acting as AML/CFT supervisors set up the necessary procedures, including through contributions from outside the profession, to achieve objective risk assessments and effective, qualitative controls.
- For the diamond sector in particular, Belgium should initiate and step up controls that factor in the high ML/TF risks of these operations, and reinforce the controllers' training and technical expertise for the supervision of diamond traders and diamond banks.
- The FSMA should carry out sufficient specific, qualitative on-site AML/CFT inspections, depending on the risks, in sectors other than that of bureaux de change. It should increase the resources allocated

to ongoing AML/CFT supervision and on-site inspections. For the insurance intermediaries sector, it should set up sufficient off-site AML/CFT supervision and on-site inspections to cater for the intermediaries' size and business volume.

- FPS Finance should implement AML/CFT supervision, including on-site inspections, in particular for Bpost operations where it acts as the central point of contact for a major European payment institution that offers money transfer services in Belgium through counter post offices. It should co-ordinate with the BNB, which is responsible for supervising the other central point of contact designated for the institution's second network of agents in Belgium.
- FPS Economy should allocate sufficient resources for ongoing supervision and on-site inspections to address the risks, and implement sufficient AML/CFT risk-based controls, especially for on-site inspections. It should also clarify the competent AML/CFT authorities for consumer credit.

Support tools for ML/TF controls

- The BNB should develop a guide for financial institutions which would provide indicators and examples of minimum requirements to mention in the annual AML/CFT report, to facilitate sector-wide and sub-sector comparisons.
- The BNB should continue its efforts to develop the periodic questionnaire so that it can be used to collect information about each institution's exposure to ML/TF risks and the effectiveness of the risk-mitigation measures applied, so that the information gathered can be used more fully as a basis for risk-based supervision.
- The FSMA should make greater use of the annual AML/CFT report and introduce effective tools for off-site supervision of intermediaries.

Co-operation mechanisms for optimising ML/TF controls

- Belgium should encourage the European Commission to consider, at European level, ways to achieve closer co-operation between competent authorities for the supervision of payment institutions conducting business in another Member State, and in particular money remittance services, under freedom to provide services.
- The CTIF and the BNB should have regular, institutionalised discussions on the ML/TF vulnerabilities, threats and risks that could have repercussions for the financial sector, and the implementation of a risk-based approach.
- The CTIF and the supervisors should work more closely together on the requirements for STRs, in order to improve their quality and help supervisors more effectively target the aspects to be controlled with regard to STRs (e.g. issue common guidelines, publish a report on the controls carried out on these aspects).
- The competent authorities should co-operate on activities that are under joint supervision by a number of them and require co-ordination to assess the risks and implement adequate controls (e.g. investment services, insurance).

Reinforcement of initiatives to promote ML/TF risk prevention

- The competent authorities should step up dialogue and discussions with the private sector on the applicable AML/CTF obligations. This would entail publishing/releasing reports on the results of off-site supervision and major on-site inspections, essentially by the BNB, and setting up regular discussion and consultation platforms, for example when guidelines are being drawn up.

Controls measures in relation to cash payment limitations

- Additional resources should be made available to FPS Economy so that it can conduct broad initiatives for sectors requiring supervision.
- The legislation should be clarified to confirm that the limitation applies to both purchases and sales of precious metals by traders (Art. 21 § 2 of the AML/CFT Law).
- Belgium should take steps to make the European Commission and the other Member States more aware of the benefits of harmonising the limitation on cash payments across Europe.

Bibliography

6

Banque Central Européenne (2014), *Liste des entités importantes soumises à la surveillance prudentielle et liste des institutions moins importantes*, Banque centrale européenne, www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm-listofsupervisedentities1409fr.pdf?48b8968851534c891be0f1a0302d6e89 (French only)

BNB (2013), *Circulaire NBB_2013_10*, BNB circular on the questionnaire and its two annexes, September 2013, www.nbb.be/pub/cp/news.htm?l=fr (French only).

BNB/FSMA (2013), *Evolutions récentes relatives à la prévention du blanchiment de capitaux*, BNB/FSMA joint circular, December 2013, BNB/FSMA, Brussels, www.nbb.be/doc/cp/fr/vo/circ/pdf/nbb_2013_16.pdf (French only)

CBFA (2010), *Circulaire CBFA_2010_09 du 6 avril 2010*, circular of 6 April 2010, CBFA, www.nbb.be/doc/cp/fr/vi/settle/circ/pdf/CBFA_2011_09-1.pdf

CBFA (2011), *Communication CBFA_2011_15 du 23 mars 2011*, CBFA, www.fsma.be/~media/Files/fsmafiles/circ/fr/cbfa_2011_15.ashx (French only)

FSMA (2013), *Respect de la législation anti-blanchiment*, Communication FSMA_2013_02, 5 February 2013, www.fsma.be/~media/Files/fsmafiles/circ/fr/2013/fsma_2013_02.ashx (French only).

Official Journal of the European Union(2013), *Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions*, Reg. 1024/2013, recital no. 29, Official Journal of the European Union, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:287:0063:0089:en:PDF>

7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings

Belgium has put in place a series of measures conducive to reinforcing the transparency of legal persons. Basic information and information on beneficial ownership on the vast majority of legal persons is publically available through the information kept by the Banque Carrefour des Entreprises (BCE), although deficiencies as regards to how current the data is are to be noted. The actions of notaries, who authenticate the majority of documents relating to the creation and lifecycle of legal persons reinforces the reliability of this information. The information available essentially gives details on the legal ownership of the company that may coincide with its beneficial ownership. Additional means exist for helping to determine beneficial ownership, namely information obtained by financial institutions and non-financial professions, including, in particular, any publically available information on Belgian listed companies as well as the information on beneficial ownership held within each non-listed Belgian company.

The competent authorities have identified some concrete ML risks and some vulnerabilities in the framework under which legal persons are organised. Nevertheless, the understanding of the risks remains sector-specific. Analysis of such risks has led to various specific measures being adopted. The recent entry into force of a certain number of them and the need for additional hindsight to be able to measure their effect mean that it is not possible to draw conclusions as to whether or not they are fully effective. The authorities are aware of the need to take further measures. The law enforcement authorities who are specialised in combatting terrorism are well aware of the vulnerabilities of legal persons to being misused for the purposes of financing terrorism, although they have not conducted any recent assessment of these aspects.

The development of legal arrangements has been limited in Belgium. For this reason, the authorities have up to now, not begun to identify and assess the vulnerabilities of these structures operating in Belgium in relation to ML. An analysis of the risk of fraud based on the use of foreign legal arrangements by physical persons subject to taxation in Belgium has nevertheless led to tightening of reporting obligations to tax authorities in regard to the existence of links to legal arrangements, including foreign ones. Professional trustees, with the exception of domiciliation companies, are covered by AML/CFT obligations.

The competent authorities in Belgium obtain required basic information and beneficial ownership information on the vast majority of legal persons set up in the country, and the information can be obtained in a timely fashion. Incoming and outgoing international co-operation relating to identifying and to exchanging information about legal persons and arrangements is generally positive.

The sanctions available for non-compliance with information and transparency obligations regarding legal persons are not fully implemented in such a manner as to be effective or dissuasive. Belgium has recently developed its arsenal of sanctions in order to mitigate the ineffectiveness of the implementation of the existing administrative and criminal sanctions. The implementation of these new sanctions is beginning to give some encouraging results.

7.1 Background and Context

(a) Legal persons

7.1. In Belgian Law, the concept of a private-law legal person extends to cover any group of individuals who come together in a common interest. Such legal persons may seek to make profits – companies – or be non-profit-making – non-profit organisations (NPOs).

7.2. Five types of company may be created in Belgium: the *société anonyme (SA)* (public limited company),¹ the *société en commandite par actions (SCA)* (company with liability limited by shares), the *société privée à responsabilité limitée (SPRL)* (private limited-liability company), the *société illimitée (SCRI)* (unlimited-liability co-operative company), and the *société cooperative à responsabilité limitée (SCRL)* (limited-liability co-operative company). Belgian legislation also makes provision for two types of partnership: the *société en nom collectif (SNC)* (general partnership) and the *société en commandite simple (SCS)* (limited partnership).

7.3. The *SPRL* is the form of company that is most common in Belgium. It is a highly accessible structure because it requires only a small amount of starting capital or seed money and a limited number of founders for incorporating it. The securities issued are mandatorily in registered form and they are transferable under specific conditions. The 'starter' *SPRL* makes provision for the amount of capital required to be as low as one euro. This form of the company was created to foster entrepreneurship and to combat the practice of setting up a company abroad with a branch being opened in Belgium. The *SA* is the second most common form of company, chosen, in particular, by large businesses insofar as the securities of this form of company are freely assignable, except in specific situations, unlike the securities of the other forms of company. Together, *SPRLs* and *SAs* account for 93% of Belgian companies.

7.4. The other legal persons are non-profit organisations (NPOs) that can be broken down into:

- Foundations (*fondations*), which may be set up for private purposes when a founder assigns an asset, an estate or some other form of wealth to a specific not-for-profit purpose (e.g. for safeguarding a collection of art works or for keeping a family concern in the family). Foundations can also be of public utility, in which case the asset, estate, or wealth is assigned to achieving a not-for-profit objective of a philanthropic, philosophical, religious, scientific, artistic, educational, or cultural nature;
- Non-profit associations, which are groups of natural or legal persons that have activities that are not carried out for profit (*ASBLs – associations sans but lucratif*), and that may be of international utility (*AISBLs – associations internationales sans but lucratif*).

7.5. Belgium has about 7 000 'large' and 'very large' *ASBLs*, *AISBLs*, and foundations, and about 128 500 'small' *ASBLs*, *AISBLs*, and foundations.

7.6. Forming *SAs*, *SCRLs*, *SPRLs*, *SCAs*, *AISBLs*, and foundations requires an authentic act or memorandum to be drawn up by a notary, who, on such occasions, conducts the due diligence required of him or her by the AML/CFT Law, on the founders and incorporators, and verifies the statutes (articles of association). In Belgium, notaries are public officers appointed by the King and who, by virtue of delegation of authority by

1 European Companies (SEs) are governed by European Council (EC) Reg.2157/2001 of 8 October 2001 on the Statute for a European Company, as transposed into Belgian Law by the RD of 1 September 2004 that permits the creation and management of companies with a European dimension, detached from the strict territorial application of the legislation on companies of the State on whose territory they are created. The rules applicable to Belgian *sociétés anonymes* apply *ipso facto* to European Companies. There were 11 SEs in Belgium in 2013.

the State, perform public-service missions and are required to see that the Law is applied properly. *ASBLs* and *SCRIs* may be incorporated by notarial act, but also by privately signed acts or memoranda.

7.7. All of these entities are required, within a time limit of 15 days, to file a copy of their memorandum/act of incorporation with the registry of the locally competent commercial court. An extract from the memorandum/deed is published in the *Moniteur Belge* (Belgian Monitor), which is Belgium's official gazette, and the entity is then registered with the BCE, which is the Belgian companies register.² Belgium has also instituted a system whereby requests for the creation of an association or business may be filed on-line (*système e-greffe*).

7.8. Any legal person governed by Belgian Law, any legal person governed by a foreign law and having a main site in Belgium, and any Belgian branch of a foreign company is required to be registered with the BCE. The requirements regarding publishing, registering, and keeping the information are identical to those for companies governed by Belgian Law.³

Table 7.1. BCE Data on Legal Persons (July 2014)

Numbers	Type
50	Co-operative companies governed by public law (under the former law)
55	Limited-liability co-operative companies governed by public law
201	Foundations of public utility
559	Limited-liability co-operative companies with a social purpose
1 013	Non-commercial companies in the form of a limited-liability co-operative company
1 037	Private foundations
2 424	Companies with liability limited by shares (SCA)
10 759	Limited-liability co-operative companies (SCRL)
16 528	General partnerships (SNC)
18 736	Co-operative companies (under the former law)
25 056	Limited partnerships (SCS)
116 437	Public limited companies (SA)
135 130	Non-profit associations (including AISBLs)
352 330	Private limited-liability companies (SRRL)

Source: BCE statistics, 30/06/2014

2 Presentation of the Banque Carrefour des Entreprises [BCE] (in French), FPS Economy, see C.24.3. The BCE contains, inter alia, information on: the name, the business or company name of the legal person, the specific designation of various addresses, the legal form and status, the date of establishment and termination of the company, identification data on the founders, delegated officers and other officers (Art. 6 of the law of 16 January 2003).

3 Belgian companies law applies to foreign companies who locate their main sites in Belgium (Art. 110 of the *Code de droit international privé* (Belgian Code of Private International Law)).

(b) *Legal arrangements*

7.9. Belgian legislation does not allow trusts to be set up. Belgium is not a signatory to the Hague Convention on the Law Applicable to Trusts and on their Recognition. However, trusts set up abroad may be recognised for legal and tax purposes in Belgium.⁴

7.10. Various mechanisms are based on the principle of trust ownership (*propriété fiduciaire*), the main one of such mechanisms being private foundations, which can perform the function of a trust (*fiducie*), even though such a legal arrangement does not exist *per se* in Belgium.

7.11. The services provided by professional ‘trustees’ are, in Belgium, usually provided by financial institutions (in their capacity as investment management companies) or by lawyers, notaries, or the accounting/tax professions, all of whom are required to comply with the obligations of the Belgian AML/CFT Law (see Section 5).

7.12. The authorities emphasised that the use of legal arrangements⁵ and of administration of foreign trusts by trustees who are residents are not common practices in Belgium. The national ML risk assessment did not identify specific risks associated with Belgian legal arrangements; however, it did point out the risks related to activities in Belgium involving trusts and companies located in financial centres with little transparency.

(c) *International context for legal persons and arrangements*

7.13. Belgium is placed well in international rankings of countries that welcome foreign investors or of those countries where it is easy to do business.⁶ This is due in part to its location, a business regulatory environment that is favourable to the establishment of companies and an attractive tax situation.

7.14. Belgium is not an international centre for setting up and administration of companies or of legal arrangements. Foreign companies located in Belgium are often commercial subsidiaries or European headquarters. The most represented international companies are from the service sector (law and audit firms, etc.) followed by the media and banking sector.

7.15. The CTIF, through its analysis work on STRs, has identified the use of complex legal structures of foreign companies and trusts. The typologies analyses of the cases transmitted to judicial authorities have been made public to aid persons and institutions covered by the law, and in particular the non-financial professions, to identify ML operations. They also identified the role played by certain tax and financial advisors in setting up fraudulent structures. These involved companies set up under Belgian law, companies and legal arrangements located abroad or even the sale of dormant companies.

7.16. At the European level, Belgium takes part in the initiatives and electronic tools that facilitate co-operation and cross-border access to information on businesses, such as the voluntary network for co-operation between European commercial registers (European Business Register – EBR). It brings together 28

4 Art. 122ff. of the Belgian Code of Private International Law and Art. 2 § 1 13 and 307 § 1, subpara. 4 of the Income Tax Code, CIR 92. (Service Public Federal Finance, nd)

5 By its Law of 30 July 2013, Belgium introduced an obligation for natural persons to declare in their annual tax returns the existence of any legal arrangement of which the taxpayer is a beneficial owner. This measure is applicable as from the tax returns to be filed in 2014 (for income received in 2013). It will make it possible, as of 2015, to have an annual estimation of the number of taxpayers who are beneficial owners of legal arrangements in Belgium.

6 *Ease of doing business index*, World Bank Website (nd)

European countries and territorial entities,⁷ giving access to data recorded in the Belgian National Register. The data available on the companies registered in the Belgian register to be cross-checked with the data of the other member of the network. Belgium also participates in the European project resulting from Directive 2012/17/EU of the European Parliament and of the Council on the interconnection of central, commercial and companies' registers.

7.2 Technical Compliance (R 24, R 25)

Recommendation 24 – Transparency and beneficial ownership of legal persons

7.17. **Belgium is largely compliant with R 24** – The authorities possess a certain level of information on the ML/TF risks associated with the categories of legal persons that can be incorporated in Belgium, even though that information could be collected and analysed in a more systematic and co-ordinated manner, and some of that information could be kept better up-to-date. As regards the information on beneficial owners, the information of the BCE or that appears in the shares registers kept by companies essentially gives information on the legal ownership of the company that may coincide with its beneficial ownership. Additional means make it possible to help to determine the beneficial owners: through the information obtained by financial institutions and non-financial professions, and in particular notaries, in the course of CDD, or any publicly available information about Belgian listed companies, as well as information on beneficial ownership maintained by each non-listed company pursuant to Art.515bis of the Companies Code. In addition, financial institutions and non-financial professions subject the information that is disclosed to them to a credibility and relevance test, and, in the event of any doubt on either of those aspects, they are bound to take any other appropriate reasonable measure to identify and to verify the beneficial owners.

7.18. Bearer securities were outlawed in Belgium by the Law of 14 December 2005 that came into full effect as of 1 January 2014. As regards nominee agreements, absence of public information on the identity of the person actually holding the share (who may be a foreign company) and of the status of the nominee makes it difficult to do any verification of the shareholder.

7.19. Legal persons (or their representatives) do not incur sanctions for disclosing erroneous or misleading information to professionals covered by the law when they are disclosing information about their beneficial owners. However, the consequences of such acts may lead to sanctions (e.g. the suspension of rights or the sale of shares pursuant to Art.516 of the Companies Code). Because no indications are provided on the sanctions policy applicable when requirements on transparency of legal persons are not complied with, it is difficult to assess how proportionate such penalties are.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

7.20. **Belgium is largely compliant with R 25** – Due to the limited development of legal arrangements in Belgium, the obligations of R 25 apply primarily to professional trustees who are subject to AML/CFT obligations. Use of trustees who are not professionals and therefore not covered by AML/CFT obligations is apparently not common practice. Financial professions and non-financial professions whose customers are legal arrangements are obliged to identify the representative or agent of the customer and its beneficial owners, and to verify their identities. The general system of sanctions applicable for failing to comply with obligations laid down by the AML/CFT Law is applicable to professional trustees, who are among those professionals covered by the AML/CFT system. There is no clear policy on applicable sanctions that would make it possible to determine whether or not such sanctions are proportionate.

7 Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Slovenia, Spain, Sweden, and United Kingdom, as well as Jersey, Guernsey, "the former Yugoslav Republic of Macedonia", Norway, Serbia, and Ukraine.

7.3 Effectiveness: Immediate Outcome 5 (Legal Persons and Arrangements)

(a) Information on Legal Persons and Arrangements

7.21. Belgium has mechanisms that identify and describe the various types, forms and characteristics of the legal persons that can be incorporated under Belgian Law. The procedures for incorporating such persons are available to the public via various Internet sites.⁸ Similar information is available for foundations and associations.⁹ There is no information available and issued by the public authorities relating to the legal arrangements that may be set up in Belgium because they are not structures that are very common in the country.

(b) Identification of the risks and vulnerabilities of legal persons

7.22. Various concrete risks and vulnerabilities in the framework under which legal persons are organised have been identified through sectoral analyses by the competent authorities and through the national ML risk assessment (see Section 1). Analysis of statistical information (such as variations in the type of companies incorporated, the periods of activity, and the mean lifespan of certain companies) has also made it possible to detect operational changes in the use of legal persons governed by Belgian Law for criminal purposes.

7.23. Identification of mechanisms through which corporate vehicles are used for criminal purposes makes it possible to understand the vulnerabilities of the Belgian system better: the Federal Police have thus detected networks through which trafficking and sales of companies are handled by certain accounting/tax professions and notaries for fraudulent activities of various types (social security fraud, bankruptcy fraud, organised VAT fraud), marketing of companies with “straw men” or front men, and numerous irregularities with regard to actual registered offices. The Federal Police initiated criminal investigations of those professionals. The authorities have also identified a range of legal and tax consultancy services for pre-incorporation and deeds/memoranda relating to the life of companies that are offered by persons who are not bound to comply with any of the AML/CFT obligations, and that are conducive to misuse of the companies that are incorporated.

7.24. The categories of legal persons, and in particular the categories of companies, that are particularly exposed to misuse have also been identified. In its 2009/2010 annual reports,¹⁰ the CTIF indicated that various types of foreign legal person appear regularly in fraudulent structures, e.g. certain companies grouped together under the generic wording of ‘limited (Ltd)’.¹¹ In June 2013, monitoring action was proposed to the College for combatting tax and welfare fraud (*Collège pour la lutte contre la fraude fiscale et sociale*) in order to reinforce monitoring and investigation of such activities. The CTIF has also observed the use of shell companies, or companies with fictitious directors and/or having vague business purposes. Criminal investigations initiated by the Prosecutors’ Offices and by the Federal Police confirm that *SPRLs* and *SAs* are clear leaders among the legal forms used by organised crime in Belgium. This observation can be explained firstly because those companies represent 93% of Belgian companies, but also, as regards *SPRLs*, doubtless because of the very accessible nature of this type of entity, further accentuated for ‘starter’ *SPRLs* for which only 1 euro in starting capital is necessary, and which are particularly vulnerable to misuse.

8 For example, Portal belgium.be (nd) (official services and information), Types of company or, FPS Economy (nd a), Creating an enterprise/Structuring your enterprise project/Forms of company.

9 For example, the notaries website, www.notaire.be/societes/asbl

10 CTIF Annual Reports, 2008 to 2012 (CTIF, nd). See also: laundering via the use of co-operative financial structures (2011), misuse of non-profit organisations (2013), use of domiciliation companies (2010).

11 Which limits the liability of the managers and shareholders to their shares in the share capital and enjoys favourable tax treatment in certain countries.

7.25. In 2011, the CTIF observed, together with the FPS Economy that business domiciliation was not only handled by chartered accountants and lawyers,¹² but also, increasingly, by domiciliation companies, without any apparent link with persons or institutions covered by the AML/CFT Law. A risk of ML was also noted for this sector, related, in particular, to incorporation of shell companies or to the location of fictitious registered offices. In June 2012, the CTIF proposed regulating these structures and bringing them into the AML/CFT. A study relating to possible means to be implemented – the draft text of which was supplied to the assessment team – was being finalised at the time of the on-site visit.

7.26. The authorities' understanding of the vulnerabilities of legal persons nevertheless remains sectoral, and is not deduced from an overall and updated assessment of all of the forms of legal persons.

7.27. Due to the limited development of legal arrangements, the authorities have, so far, not initiated actions to identify and to assess the vulnerabilities of the legal arrangements operating in Belgium. The recent amendment to the Income Tax Code imposes an obligation on Belgian taxpayers who are physical persons to report their links (as founder or beneficiary) with a legal arrangement, including a foreign one. This amendment is however the result of an analysis of the risk of fraud that is related to use of foreign legal arrangements (see R 25.5).

7.28. The prosecution authorities who are specialised in combatting terrorism are aware of the vulnerabilities of legal persons to being misused for TF purposes, although they have not conducted an assessment of the TF risks associated with the various forms of legal persons. They do however carry out ongoing monitoring of activities and transactions of legal persons that are identified to be at risk. The authorities provided information showing that, several years ago, they undertook targeted actions in the NPO sector. The authorities indicated that they continue to pay particular attention to this point, in particular depending on the activities of the NPOs (see Section 4).

(c) Measures aimed at preventing the use of legal persons and arrangements for ML/TF purposes

7.29. The authorities have taken a number of legislative and operational steps to prevent the misuse of legal persons and legal arrangements for ML/TF purposes (see R 24 and R 25). Among these it is important to note in particular the elimination of bearer shares, which became fully effective on 1 January 2014, as well as the procedure for automatic removal from the register (see below).

7.30. The authorities have also undertaken awareness-raising with stakeholders, and particularly with financial institutions and notaries to ensure that they pay particular attention to business conducted with certain types of legal persons. The representatives of the private sector who were met confirmed that, in practice, credit institutions and non-financial institutions are particularly watchful on entering into business relations with certain types of customers (e.g. offshore companies, companies with complex ownership chains and having links with countries having advantageous taxation, and *Stak* governed by Dutch Law¹³ for succession planning). Risk profiles have been established for certain forms of company, and for certain target sectors whose activities have been identified (e.g. construction, a sector handling cash). In their sector-specific AML/CFT regulations, the CTIF and the professions have developed specific and non-exhaustive indicators of suspicion for ML activities linked to the use of legal persons and legal arrangements. This approach has made it possible to identify risk situations requiring the watchfulness and due diligence of the professions to be reinforced.

7.31. Inspections are regularly implemented by the FPS Economy in order to identify 'dealers in companies' making use of front men. A blacklist of people suspected of being involved in such dealings is published regularly. An investigation by the Economic Inspectorate (*Inspection Économique*) on the role of fraud facilitators who supply ready-made or off-the-shelf companies (generally *SPRLs* or "starter" *SPRLs*) to

12 Contravening, for these professionals, the rules by which their professions are organised.

13 Hoegen Dijkhof, Dr Hans J. (2013).

fraudsters, using front men, was in progress at the time of the on-site visit. The tax authorities also conducted inspections targeting limited-liability companies over the period 2007-2009, as a pilot action, and then again in 2013.

(d) Access, reliability and accuracy of basic information and of information on the beneficial ownership of legal persons

7.32. Basic information and, to a certain degree, on the beneficial ownership of legal persons registered in Belgium is accessible mainly via the companies/business register, i.e. the BCE. Essentially it contains information on the legal ownership of the legal persons; this may also be used to gain information on beneficial ownership.

7.33. Other mechanisms also help competent authorities to determine beneficial ownership:

- Use of existing information, in particular information obtained by financial institutions and DNFbps, which are required to identify and verify the identity of beneficial owners (Art. 8, AML/CFT Law). Such information must be provided by the customer, and the financial institution/DNFbp then applies the information to a credibility and relevance test.
- Use of information available on large shareholdings in non-listed companies that have issued dematerialised shares; such information is available starting from the threshold of 25%.
- Use of available information on Belgium listed companies indicating share holdings larger than 5%.

7.34. Incorporating or setting up the vast majority of companies, foundations, and *AISBLs* in Belgium, which are recorded in the BCE, requires an authentic act or memorandum drawn up by notary. In the notary's capacity as an authenticating civil servant, the notary can be held liable as to the correctness of the information mentioned in the acts. On drawing up such acts or memoranda, notaries are required to verify the statutes or articles of association and to identify and verify the identities of the incorporators (founders and persons who hold shares). The notaries met with indicated that they check the veracity of the declarations that are made to them not only through the production of supporting documents (identity documents, statutes, etc. see C.10.3), but also on the basis of the consistency and likelihood of the project explained to them, depending on the client profile, his/her environment, etc. When doubts exist as to the truth of the client's status, for example, the notaries interviewed indicated that they meet the client face-to-face and question him/her directly about the project and its objectives, in order to grasp the rationale lying behind it. When the statutes of a legal person are pre-drafted by consultants/lawyers (trust, tax, or accounting/tax consultants/lawyers), they are verified with increased diligence by the notary, in particular if the notary does not know the consultants/lawyers. In addition, the main changes in the lifecycle of companies – amendments to the statutes, changes in the structure, etc. – must also be established and verified by a notary. The information is also forwarded to the registry of the commercial court and published in the *Moniteur Belge* (Belgian Monitor) and in the BCE. It should be noted that assignments of shares are not operations that have to be authenticated by a notary, and they are not therefore mandatorily published and indicated in the public registers. However, they do appear in the register of shares and bonds that the company is required to maintain. Assignments of shares of jointly and severally liable partners in partnerships are published officially.

7.35. The vast majority of financial institutions and DNFbps met indicated that, in practice, they mainly use private databases for determining beneficial owners, such databases affording ease of access to updated and consolidated information. This also enables them to mitigate the insufficiencies of the data in public registers and to supplement the information to which they have access through their (future) customers themselves. In view of the cost involved for these checks, certain professional associations have made free access to certain private databases available to their members. The professionals indicated that they also cross-check information with existing customers or exchange with other financial institutions while complying with data protection measures. By way of example, it was indicated that there were difficulties in determining beneficial owners when they had connections with other countries and when there were chains of entities with complex legal constructions or arrangements. In such situations, and when there is any doubt about the ultimate beneficial owner of the legal person, the financial institutions and DNFbps interviewed all indicated that they refuse the business relationship. It should be mentioned, in this context, that the BNB

7

conducted a horizontal initiative to check on identifying/verifying beneficial owners in 2012 and 2013 with all of the financial institutions that it supervises. This was following a deadline provided by the AML/CFT Law for the implementation of the new requirements introduced in 2010. The initiative was conducted in the context of an off-site inspection and led to remedial actions in the form of 'serious administrative measures' (correspondence imposing deadlines for taking remedial action and development of corrective action plan) for 14 credit institutions and 9 insurance companies (on the basis of provisions of inspection laws).

7.36. The data held by financial institutions and DNFBPs on beneficial owners would appear to constitute the main source of information for the Belgian authorities. However, that statement should be nuanced, because checks for information on the beneficial owner of a suspicious entity by the competent authorities, be it by FIU, or by some other investigation and law enforcement authority, depend on the case, on the type of company in question, Belgian or foreign, and on the information already available in the databases of the national authorities, etc.

7.37. As regards Belgian companies, the CTIF has access to the BCE that is direct and free of charge, and that is more extensive than the access available for the general public.¹⁴ In addition to consulting that database, the CTIF has pay access to a commercial database. Since 2009, public prosecutors and investigating judges have had access to the information contained in the BCE, and that access was broadened in 2014. Various searches are possible by crossing-checking information available in the National Register¹⁵ and in the BCE.

7.38. Generally, the administrative and judicial authorities feel that they obtain in a timely fashion both basic information and beneficial ownership information of a satisfactory quality. This is in spite of having to use, depending on the needs of the investigation, different channels to obtain it. The private sector discloses information in due time and within the time limits set by the requesting authority. Whenever necessary, the information is collected directly from and/or verified directly with the companies. The work of investigators is made more difficult however by the lack of technical resources and software that would enable them to cross-check existing data (data mining). At the time of the on-site visit, the police no longer had access (for two years) to the database of a company specialised in searching for information on legal persons, since the public contract in question and the award decisions are the subject of legal proceedings.

7.39. For entities registered abroad, the information sources mainly used by the Belgian authorities are the public companies/business register of the country in question, information disclosed following requests made to foreign police authorities or to foreign FIUs, and information from foreign tax authorities. Co-operation through the CTIF is used effectively by the Belgian authorities.

7.40. Belgium is aware of the need to take corrective measures in order to improve the reliability of the information available in the public registers and databases.

- Actions were planned for raising the awareness among the registries of the commercial courts of the problems of quality and lateness of entering the data into their registers and databases. A certain amount of lateness was also observed in the transmission by the registry of the commercial court to the BCE of the amendments filed (in particular, address, directors, manager, business name), and in the absence of a strict time limit within which such amendments should be transmitted.

14 The search possibilities are very broad and searches can be made either on the data of the company itself, or on the basis of the identification of a physical person, all of whose connections to any Belgian company(ies) can then be established. Large numbers of details are then available on the companies (registered office, VAT No., site unit, all of the directors/managers (present and past), declared business activities, information as to any bankruptcy, etc.), and direct links appear to various 'external sources', mainly a link to all of the acts relating to the company that have been published in the *Moniteur Belge* and to the *Centrale des bilans* (Balance Sheet Centre) on the website of the BNB that gives direct access to the annual accounts of the company.

15 The National Register is an IT system for recording, storing, and disclosing information on the identification of physical persons. See C.10.5. Service Public Federal Interieur (nd).

- As regards the BCE, already, since 2011, a specialised unit had been put in place to co-ordinate the quality control of the recorded data by the business formalities centres of the FPS Economy, who are responsible for collecting the data on legal persons and of recording it in the BCE. Access to the database of the BCE has been improved and the list of accessible data has been enriched, including the search functions. The authorities have updated the data by deleting a large number of inactive or dormant companies on the basis of the administrative deregistration procedure adopted in July 2013 (see Section 7.1). The strategy committee of the BCE had just been set up at the time of the on-site visit and will continue initiatives to improve the quality of the data accessible via the BCE. Nevertheless, the BCE remains dependent on the resources available to it to be able to update the database effectively. Various reports from the authorities mention the difficulties that the BCE has in optimally processing the influx of information, in particular notifications of judgements and rulings¹⁶ and other amendments and de-registrations following observations made by the authorities (police, economic inspectorate, public prosecutors' offices).

7.41. Finally, it is regrettable that Belgium has still not set up a central criminal records system for legal persons, although it is foreseen in the Law of 4 May 1999 on criminal liability of legal persons (see Section 3). Therefore, there is no centralised access to information on any criminal convictions, probations and suspensions in reference to legal persons. Furthermore, the absence of reliable statistics on these aspects means that it is not possible to gain insight to the crimes committed by legal persons and consequently the orientation to take as far as a general policy on this issue.

(e) Sanctions

7.42. It should be noted that the first "sanction" for lack of transparency is the impossibility of continuing a project to set up a company or to establish a business relationship if the persons in charge of collection and oversight of the information are not satisfied that the information is conclusive, likely, and consistent.

7.43. Although sanctions exist for entering false information, the Belgian authorities are aware that the system of sanctions/penalties for persons who do not comply with the transparency obligations incumbent on legal persons is neither effective nor dissuasive. This is evidenced by the failure of the various competent authorities to apply sanctions, or, in the rare cases when application proceedings have been implemented, by the lack of follow-up both by the public prosecutors' offices and at the level of actual collection of the fines imposed. The established lack of resources at both human and technical (IT) levels has a definite impact on these aspects. Public prosecutors admit they are incapable of giving sufficient priority to investigations/prosecutions for certain acts through lack of resources. This concerns, for example, cases of lack of qualifications required for the directors who are managers, or investigations into fictitious registered offices. In the past, before their capacity declined, certain public prosecutors' offices questioned the directors or managers of companies who did not file their annual accounts, and, either the situation was remedied and a criminal-law settlement was proposed, or the companies were ordered to be wound up. There are no statistics as to the number of court-ordered dissolutions that were ordered. Since the Belgian legislator has, since 2005, decriminalised non-filing of annual accounts with the BNB, the priority given to this subject in the public prosecutors' offices has declined. However, some examples were given of proactive search policies followed by some public prosecutors' offices, with the assistance of the local police, for combatting fictitious or dummy registered offices.

7.44. In order to mitigate the ineffectiveness of implementation of the existing administrative and criminal sanctions and penalties, Belgium has put new procedures in place. The procedure for automatically deregistering companies from the BCE register has started to give concrete results. In 2013, 96 093 businesses were administratively deregistered following the absence of filing of their annual accounts for three consecutive years, and 4 796 were deregistered during the 1st half of 2014. That represents about 20% of all of the legal persons registered, and confirms that the reforms put in place should be implemented as quickly as possible in order to reinforce the reliability of the BCE tool. Other procedures recently put in place had not yet been used (e.g. deregistering companies on the basis of a combination or accumulation of criteria) in the

16 Conseil d'État (2003), Art. 23.

absence of implementation procedures, or had been used only to a very small extent (e.g. criminal sanctions). The procedure put in place by the new Code of Economic Law (*Code de Droit Economique*), in force since February 2014, and enabling the administrative authorities to propose administrative settlements had not yet been applied at the time of the on-site visit. The action plan for a more appropriate system for collecting payment of criminal fines, which was adopted by the Belgian Cabinet in July 2014, will also constitute positive progress once it is actually implemented.

(f) International co-operation for requesting and granting appropriate assistance in matters of identification and of exchange of information on legal persons and arrangements

7.45. Firstly, it should be recalled that basic information relating to legal persons and certain legal arrangements is available on line and in several languages,¹⁷ which can enable foreign authorities to continue their investigations without necessarily having to wait for a reply from the Belgian authorities. International co-operation, both incoming and outgoing, on identification and exchange of information on legal persons and arrangements seems to be operating well, apart from a few exceptions.

7.46. *Requests addressed to Belgium:* Belgium is capable of providing very broad international assistance. At the request of a foreign authority, the competent Belgian authorities make full use of their competences and powers of access to gather the requested information in a timely fashion and to supply it to the requesting authority (see Section 8 on all of these aspects).

7.47. The replies from the countries asked for feedback on international co-operation with Belgium did not raise any particular difficulties as regards the quality of the information received on legal persons, or the timing delay for the response. The competent Belgian authorities confirmed that they gather basic information and beneficial ownership information in a timely fashion on the vast majority of legal persons set up in the country. However, the reservations expressed above regarding the quality of the information that is kept on Belgian legal persons or legal persons operating in Belgium raise questions about the capacity of Belgium to supply fully reliable and up-to-date information to foreign authorities on these aspects. At the time of the visit, Belgium had not put in place regular monitoring of the quality of the assistance given to foreign authorities relating to legal persons and arrangements.

7.48. *Requests sent by Belgium:* As regards legal persons governed by foreign law, the public prosecutors indicated that they are entirely reliant on police information obtained through international co-operation or through letters rogatory sent to their foreign counterparts. The absence of statistical information on the frequency with which mutual assistance or police co-operation is used, as well as of concrete case examples, leads to the conclusion that there is no proactive approach for regular and fully effective use of these channels by investigative and prosecution authorities. This is the case in spite of the absence of legal obstacles. The competent authorities indicated that they were satisfied with the international assistance received from foreign authorities, with a few notable exceptions, in particular in the context of mutual legal assistance with certain States, including member States of the EU (e.g. the United Kingdom, the Netherlands), and certain jurisdictions, in particular in the Caribbean area. It has happened that legal proceedings instigated for ML could not continue through failure to receive the necessary information from abroad.

7.49. As for international co-operation with other FIUs, it was observed that the quality of information obtained by the CTIF on legal persons and arrangements had improved after a targeted approach was applied. This approach aimed at providing more context for the questions in the request. The CTIF was able, on the basis of concrete cases, to demonstrate that it had obtained useful information on beneficial ownership and legal persons located abroad in cases with an international dimension or complex structures.

7.50. ***In conclusion***, the authorities' understanding of the vulnerabilities of legal persons remains sectoral, and is not deduced from a continuous, overall and updated assessment. The law enforcement authorities who

17 For example: FPS Economy website, European Business Register. FPS Economy (nd b).

are specialised in combatting terrorism are aware of the vulnerabilities of legal persons to being misused for TF purposes and carry out ongoing surveillance depending on the case, although they have not conducted any recent assessment of these aspects.

7.51. Competent authorities have identified concrete ML/TF risks and vulnerabilities in the framework of legal persons. Several initiatives have been taken with a view to addressing them; however the recent entry into force of certain of these measures and the need to have more hindsight to fully appreciate their effects means that they cannot yet be considered fully effective. The authorities are aware of the need to take additional steps.

7.52. Basic information and information on beneficial ownership for the vast majority of legal persons is publicly available through information held by the companies register – BCE – although shortcomings should be noted, in particular regarding the reliability of the data and whether they have been updated. Nevertheless, the role of notaries in authenticating the majority of acts relating to the creation and lifecycle of legal persons reinforces the reliability of this information. The information available essentially provides information on the legal ownership of the company, which can coincide with the beneficial ownership. Additional means exist to help in determining beneficial ownership, in particular information obtained by financial institutions and DNFBS or any information publicly available on listed or non-listed Belgian companies. The investigation and prosecution authorities did not provide sufficient qualitative information to permit an assessment of ML/TF investigations targeting legal persons or in those where information on beneficial ownership had been sought for and timely accessed.

7.53. Since the sanctions available for punishing persons who do not comply with information and transparency obligations for legal persons are not fully effective or dissuasive, Belgium has developed its arsenal of sanctions in order to mitigate the lack of effective implementation of administrative and criminal sanctions, and the implementation of these new sanctions is beginning to give some encouraging results.

7.54. The development of legal arrangements has been limited in Belgium. For this reason, the authorities have up to now not begun to identify and assess the vulnerabilities of these structures operating in Belgium in relation to ML. An analysis of the risk of fraud based on the use of foreign legal arrangements by physical persons subject to taxation in Belgium has nevertheless led to the tightening of reporting obligations to tax authorities in regard to the existence of links to legal arrangements, including foreign ones. Professional trustees are generally covered by AML/CFT obligations.

7.55. International co-operation, incoming and outgoing, in relation to identification and exchange of information on legal persons and arrangements seems to work well.

7.56. **Belgium has achieved a moderate level of effectiveness for Immediate Outcome 5.**

7.4 Recommendations on Legal Persons and Arrangements

- The competent authorities should improve their knowledge of the risks and vulnerabilities of all of the forms of legal persons and arrangements in the country, including the type of crime committed by legal persons, by developing a horizontal analysis of these aspects, and by deepening and updating the aspects related to TF risks.
- Belgium should fully implement the measures already identified, in particular relating to the rules applicable to professionals involved in acts relating to the lifecycle of companies (e.g. services being offered by intermediaries who are not bound to comply with AML/CFT obligations, domiciliation companies), as well as in the area of sanctions.
- Belgium should consider whether it would be appropriate to extend the scope of the information collected by the existing public registers, when necessary, so as to fully include and verify information on the beneficial ownership of legal persons.

- Belgium should use the recorded data more effectively, in particular by making sure that the competent investigation authorities have the capacity and the resources necessary to enable them to do cross-checks with the existing data (data mining).
- Belgium should, without delay, put in place the criminal records system for legal persons, as provided for in the legislation of 1999.
- Belgium should continue to reinforce the reliability and the updating of the relevant information on legal persons in the public registers of the court registries and of the BCE, and on legal arrangements, in particular through measures aimed at reviewing the registration procedures; to introduce strict deadlines for the submission of information on the changes to the company; to review the aspects of oversight of the essential data supplied and of the appropriate means and resources of the competent authorities.

Bibliography

Banque Carrefour des Entreprises [BCE] (nd), http://economie.fgov.be/fr/entreprises/bce/#.VS3uYfmUf_F, accessed December 2014.

CTIF (nd), Rapports Annuels, CTIF, Brussels, www.ctif-cfi.be/website/index.php?option=com_content&view=article&id=200&Itemid=76&lang=fr

Conseil d'État (2003), Loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, 16 January 2003
www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2003011634&table_name=loi

FPS Economy (nd a), *Créer une entreprise*, Creating an enterprise/Structuring your enterprise project/Forms of company, http://economie.fgov.be/fr/entreprises/vie_entreprise/Creer/#.VS3yI_mUf_F

FPS Economy (nd b), Public Search, http://economie.fgov.be/fr/entreprises/bce/pub/PuS/#.VS32c_mUf_H

Hoegen Dijkhof, Dr Hans J. (2013), *The Dutch Foundation*, Intax Info, 20 September 2013, www.intax-info.com/index.php?option=com_content&view=article&id=1896%3A2013-09-18-10-48-04&catid=4%3Aarticles&Itemid=33&lang=en

Portal Belgium (nd), *Types de société*, Types of companies, www.belgium.be/fr/economie/entreprise/creation/types_de_societe/

Service Public Federal Finance (nd), Code des impôts sur les revenus 1992 - (version historique), Fisconetplus, <http://ccff02.minfin.fgov.be/KMWeb/document.do?method=view&id=112d14a4-998f-4c93-9c01-7e8031923abd#findHighlighted>,

Service Public Federal Interieur (nd), Direction générale Institutions et Population, www.ibz.rrn.fgov.be/fr/

World Bank Website (nd), *Ease of doing business index*, World Bank, <http://data.worldbank.org/indicator/IC.BUS.EASE.XQ>



8. INTERNATIONAL COOPERATION

Key Findings

Belgium provides assistance to countries who request it, and the Belgian authorities regularly ask their foreign counterparts for information and evidence. **The countries that gave input on the international co-operation of the Belgian authorities** (speaking broadly) **found it to be generally satisfactory**. Conversely, Belgium is generally satisfied with the co-operation that it receives, even if some requests were not responded to, in particular in determining the beneficial owners of certain foreign legal persons or arrangements.

The co-operation of the FIU with its foreign counterparts seems appropriate and effective.

On the basis of the information, including statistics, supplied by the judicial authorities, it is not possible to determine the volume of international co-operation (including extradition) dedicated to AML/CFT, and how requests for co-operation are received. The judicial authorities were not even able to indicate (i) the number of incoming and outgoing requests for mutual assistance that specifically concern ML and TF, and (ii) among those requests, which are more particularly concerned with identification, seizing and confiscation of criminal assets.

The Belgian authorities do not apply an asset sharing policy, but sharing does take place in practice on an *ad hoc* basis.

8.1 Background and Context

8.1. International co-operation plays a particularly important part in the context of AML/CFT in Belgium. Through its size and its position at the heart of Western Europe, Belgium and its population centres are readily accessible from abroad. The country is a trade crossroads and a transit country for people, goods, and services. The financial sector is dominated by multinational financial groups, and many financial services providers of the EEA trade and do business in Belgium on the basis of the European passport (see Section 5). Processing of ML and TF files, both by the courts and by the CTIF, relies heavily on the quality of the international co-operation that the Belgian authorities are able to receive from their foreign counterparts.

8.2. The bordering countries are Belgium's main partners (the Netherlands, Germany, France, Luxembourg, and the United Kingdom). FPS Justice is the central authority in Belgium for mutual legal assistance (including extradition). Since Belgium is a member of the EU, its competent authorities take advantage of the European mechanisms that facilitate direct co-operation (e.g. the European arrest warrant¹ that simplifies and accelerates certain legal proceedings). It should also be emphasised that the CTIF plays an essential part in the exchanges of information related to AML/CFT. Finally, since Belgium is a country in which layering predominates according to the national risk assessment, incoming international co-operation is significant.

8

8.2 Technical Compliance (R 36 – R 40)

Recommendation 36 – International instruments

8.3. Belgium is compliant with R 36 – Belgium has ratified all of the necessary Conventions.

Recommendation 37 - Mutual legal assistance

8.4. **Belgium is largely compliant with R 37** – Belgium has a legal database that enables it to rapidly supply the widest possible range of mutual legal assistance for investigations, prosecutions, and related proceedings in cases of ML, related predicate offences and TF. FPS Justice is the central authority for international co-operation on criminal law matters for requests concerning countries outside the EU; requests coming from EU countries are transmitted directly between judicial authorities, and FPS Justice should be informed of such requests. The systems put in place for recording the outgoing or incoming requests for mutual assistance do not allow for the possibility to track or check proper performance of letters rogatory or to measure the execution times of the requests. Thus, there are no procedures for establishing priorities for the requests.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

8.5. **Belgium is largely compliant with R 38** – Belgium has the power to take expeditious actions in response to requests from foreign countries to identify, freeze, and confiscate: laundered assets; proceeds of ML, predicate offences and TF; instrumentalities used in or intended for use in such offences; or assets of corresponding value. Since Belgian criminal law does not allow a person to be punished by confiscation without prior conviction, Belgium cannot provide assistance for requests for non-conviction-based confiscation. In addition, certain EU provisions on simplifying exchanges between asset recovery offices have not yet been transposed into Belgian law.

1 Between the Member States of the EU, the European arrest warrant (EAW) replaces extradition policy procedures with a purely judicial procedure. Each national judicial authority in the EU must recognise – *ipso facto* and with minimum checks – a request for surrendering a person that is formulated in this manner by the judicial authority of another Member State.

Recommendation 39 – Extradition

8.6. **Belgium is largely compliant with R 39** – Belgium can execute requests for extradition in matters of ML and TF. Co-operation at European level is based on the law regarding the European arrest warrant, and, outside the EU, it is the conventional principles of extradition that apply. The authorities do not have a system for recording and monitoring extradition requests that makes it possible to track, monitor, and prioritise execution of extradition requests (see R 37). Belgium does not extradite its own nationals outside the EU. The authorities indicate that the proceedings will ‘in principle’ be initiated when the requesting State has signed a bilateral extradition agreement with Belgium. Belgium may thus refuse to extradite its nationals (outside the EU) without undertaking to prosecute the offence for which extradition is sought.

Recommendation 40 – Other forms of international co-operation

8.7. **Belgium is largely compliant with R 40** – The competent authorities can rapidly agree to provide the widest possible international co-operation in matters of ML, related predicate offences and TF. The CTIF, the Federal Police and AGDA have clear procedures for transmitting and executing requests for information, and systems for establishing priorities and facilitating exchanges. The other authorities (BNB, FSMA) also have a legal framework that enables them to exchange information with their foreign counterparts, but they have not developed procedures to that effect. It was not established that FPS Economy and FPS Finance (apart from the AGDA) have a legal basis for international co-operation.

8.8. As regards indirect exchanges, there is no legal provision enabling such exchanges to take place by the CTIF even though the authorities indicate that such exchanges are possible. For the other competent authorities, no provision is made for any mechanism with non-counterpart foreign authorities.

8

8.3 Effectiveness: Immediate Outcome 2 (International Co-operation)*(a) Investigations and exchanges of intelligence in matters of ML and TF*

8.9. **The CTIF frequently exchanges information with its counterparts**, such information then being usefully incorporated into its analyses and bringing added value to the transmissions made to the judicial authorities, even if the quality and the contents of the information that the CTIF can obtain from the other FIUs are very variable. The CTIF encounters only very few problems as regards exchange of information and dissemination of information to the prosecution authorities.

8.10. As regards information supplied by the CTIF, the opinions of countries who have provided their assessments,² including major partners such as France, Germany or Luxembourg, are positive. The CTIF also supplies relevant information to its counterparts in an unsolicited and spontaneous manner. A partner thus indicated that the exchanges with the CTIF were clear and constructive and brought high added value, as illustrated by the fact that about sixty files are opened every year on the basis of information provided by the CTIF. The CTIF indicated that it has never refused to assist a counterpart, and the responses are given in timely manner, the lead times being in the range a few days to a few weeks for the more extensive investigations.

8.11. The statistics provided by the CTIF in the table below clearly indicate that it uses the exchange of intelligence in a very dynamic manner, because it sends many more requests than it receives, above all to the EU, but also to other regions, including to non-typical partners (such as the countries of Central Asia, for example).

2 Members of the FATF: Germany, Australia, Canada, Russian Federation, Finland, France, Mexico, Luxembourg, Portugal, Sweden; members of the Asia Pacific Group: Macao, China; Philippines; Vietnam; members of MONEYVAL: Armenia, Cyprus, Malta, Slovenia.

Table 8.1. Requests for assistance sent and received by the CTIF

	2008	2009	2010	2011*	2012	2013
Number of requests sent*	2 720	2 808	2 457	1 376	1 639	1 319
Number of requests received	358	402	381	420	464	536

Source: CTIF

*Up until 2010, requests for intelligence sent via FIU-NET were counted in terms of number of players involved. Since 2011, requests sent via FIU-NET have been counted in terms of number of files (in any one file, several players may be involved).

8.12. The various **police, AGDA, and intelligence services** also frequently use international co-operation, whether it be for ML and related predicate offences or for TF, and whether it be via official forums or organisations (e.g. Europol, Police and Customs Co-operation Centre (PCCC), Interpol), or informal forums or organisations (AMON – Anti Money Laundering Operational Network – for the Police). However, it should be noted that a large proportion of the exchanges made by the police take place for investigations initiated by a public prosecutor or by an investigating judge (since, by nature, purely police investigations last for a very short time in Belgium, because it is the public prosecutor or the investigating judge who directs investigations).

8.13. A certain number of cases have also given rise to transmission of files to law enforcement authorities of other countries (especially neighbouring ones) in cases of possible ML linked to the predicate offences of misappropriation of corporate assets, breach of trust, corruption, tax fraud, narcotics trafficking, etc. (at least 40 cases since 2010).

8.14. The competent authorities have a quite broad access to relevant information, in particular in terms of identification of the beneficial owners, and that information is exchanged with foreign counterparts (see Sections 3 and 7, for example, CTIF can obtain information from persons and institutions covered by the AML/CFT Law).

8.15. **The evaluation of mutual legal assistance is based primarily on qualitative data; however the quantitative data provided was also taken into account.** Incoming and outgoing mutual legal assistance is difficult to evaluate quantitatively in the absence of centralised and full information (above all in terms of statistical data), due, in particular to the fact that mutual legal assistance is the competence of various different authorities (FPS Justice, Federal public prosecutor's office, public prosecutors' offices, investigating judges), each of whom has, to various degrees, certain information, and to the fact that those authorities. Thus, statistics on international letters rogatory sent and received only include those for which the processing exceeds EUR 2 500, which is rarely the case for outgoing requests (the eventual costs of translation or travel for the official are rarely that high). However, since 1 January 2013, a statistical database has been in place at FPS Justice for requests with countries outside the EU. That database does not reference the requests transmitted directly between judicial authorities in the EU zone, insofar as the prosecutors and investigating judges only rarely inform the central authority of requests processed directly by them, in spite of the obligation to do so.

8.16. It was not possible to evaluate what becomes of requests for mutual assistance, in particular as regards identification, seizure, and confiscation of criminal assets, be it in Belgium or abroad. Finally, the Belgian authorities were not able to provide information in the form of statistical data demonstrating sharing of assets, as provided for by the Belgian legislation, and as regularly implemented in practice. The same applies for assets confiscated and repatriated following international co-operation. Only three examples were mentioned of confiscation in Belgium or at Belgium's request with sharing of assets, one of which took place in 2010.

8.17. On the basis of the observations made by the assessors, and of the contributions from the partners, **international co-operation in combatting terrorism and TF is generally effective.** The Belgian authorities indicate that international co-operation 'brings the expected added value', i.e. it makes it possible for definite progress to be made on investigations. The existence of specialised teams and authorities, at all levels (justice, police, intelligence services), the specifics of the subject (the various States concerned co-

operating, according to the authorities met, more rapidly and more effectively than on ordinary law matters) are important factors in this analysis. A lack of resources, both human and technological (in particular as regards the computer system), was pointed out to the assessors – a lack that, without directly adversely affecting investigations as things currently stand, is not without repercussions on the effectiveness of the system and particular attention should be paid to it by the competent authorities.

(b) Mutual legal assistance provided by Belgium

8.18. It can be concluded, based on the opinions given by various countries (representing several hundred requests) and on the interviews conducted with the representatives of the competent Belgian authorities, that **Belgium provides assistance that is satisfactory or indeed good in the field of international mutual legal assistance on criminal law matters**. Certain partners indicated that the assistance provided by Belgium was of very high quality, and several also indicated that communication was easy, one partner noting the efforts made by the Belgian authorities to adapt to the required formalities. As a positive example of international co-operation, the Brussels public prosecutor's office has a specific department responsible for international co-operation. In addition, certain judicial districts in border areas have developed excellent contacts with their foreign neighbours.

8.19. It appears that this assistance is provided in a timely fashion by the Belgian authorities, according to certain foreign authorities who asserted that the mutual assistance and extradition are provided within times ranging from 3 to 10 months. None of the countries who gave opinions noted any refusal to grant mutual legal assistance (or extradition). The Belgian authorities have quite wide access to relevant information, in particular in terms of identifying the beneficial owners (see Section 7).

8.20. In terms of **extradition**, ML/TF cases are processed like any other request: while the surrender system instituted by the European arrest warrant is, in the opinion of professionals, generally effective, doubts remain as to the effectiveness of extradition outside the EU, particularly in terms of the length of the procedures. In addition, it is not established that Belgium initiates proceedings against its own nationals when extradition has not been granted. The Belgian authorities indicate that the main reasons are the wording of the underlying treaty (which does not always make provision for that possibility), the lack of reciprocity or of collaboration by the counterparty for establishing the facts, the lack of double criminality, or the lapsing of the statute of limitations for taking action.

8.21. Finally, the Belgian legislative framework does not make it possible to grant assistance, as required by the FATF, for co-operation requests based on confiscation procedures without prior convictions (at least in certain circumstances, such as death or absconding of the perpetrator of the offence), which, depending on the circumstances, can adversely affect the AML system. In practice, no partner of Belgium raised this point.

(c) Mutual assistance requested by Belgium

8.22. According to the interviews during the on-site visit, the Belgian judicial authorities, in particular the investigating judges, regularly use mutual assistance in all ML and TF cases.

8.23. In the opinions of the professionals met, mutual assistance in criminal law matters works quite well at EU level, in particular because of the specific regulations and mechanisms (e.g. the European arrest warrant). Outside the EU, the authorities assert, in general, that they do not encounter problems as regards the countries in which the amount of exchange of information and of provision of assistance is highest on AML and CFT matters, while, at the same time they regret the lengthiness of the procedures, ranging in general from 6 months to 2 years for execution of a request for mutual assistance. Co-operation remains difficult with a limited number of jurisdictions, in particular in cases of ML and predicate offences committed in the diamond sector even though the amounts involved are large.

8.24. The Belgian authorities also regularly use organisations responsible for co-operation and co-ordination at European level, such as EUROPOL and EUROJUST. In addition, Belgium regularly participates in joint investigation teams (particularly in cases of organised crime or narcotics trafficking, which may lead to ML).

(d) Other competent authorities

8.25. The BNB and the FSMA have legal tools enabling them to co-operate with their counterparts in performing the AML/CFT missions entrusted to them. The BNB often uses such mechanisms because of the cross-border activities of a large number of establishments that it has to oversee. The essentially domestic activity of the establishments placed under the oversight of the FSMA means that it uses these mechanisms less often.

8.26. The main focuses of international co-operation for the BNB are firstly its participation in a European college of supervisors set up to monitor banking groups with operations in several countries of the EU (see Section 5, and R 40), and, secondly, the exchange of information and co-operation on a bilateral basis, in the event of common interest relating to the activities of a financial institution or in the event of cross-border activities.

8.27. The FSMA indicates that it co-operates with its foreign counterparts to identify persons who act as financial intermediaries in Belgium, without being authorised to do so. Such persons are often businesses of foreign origin, and the supervisory authorities of those countries warn and refer the matter to the FSMA who, although it is not empowered to intervene on the premises of such service providers, can publish warnings to the public on its website (see Section 5 and R 40). The FSMA cites an example of co-operation to that effect with the British Financial Services Authority. The BNB and the FSMA indicate that they also co-operate with their foreign counterparts to verify the fitness and properness of the managers and shareholders (see Section 6). The FSMA indicates that, in general, few situations require international co-operation.

8.28. ***In conclusion***, the international co-operation provided by Belgium is considered to be of good quality by its partners. No country indicated any major difficulty with Belgian practices in matters of exchange, and the assessors did not have any information that might suggest that the Belgian system of international co-operation suffers from any serious deficiencies as regards effectiveness. This observation was confirmed by the interviews conducted with the representatives of the various competent authorities. This observation was particularly positive in matters of combatting TF and terrorism. The legal limitations observed do not, in practice, seem to have any preponderant impact on exchange of intelligence.

8.29. **Belgium has achieved a substantial level of effectiveness for Immediate Outcome 2.**

8.4 Recommendations on International Co-operation

8.30. In order to enable appropriate policies to be in place, conducive to reinforcing and to improving the effectiveness of Belgium's international co-operation on ML/TF matters and more generally to reinforcing and improving the effectiveness of the combat against those crimes, Belgium should:

- Equip itself with appropriate IT tools to enable the judicial authorities, at all levels of the proceedings, to have an overall vision of mutual assistance for criminal law matters, and analyse the effectiveness of the system in order to mitigate any deficiencies that might remain, improve the processing of the requests and find the appropriate solutions with respect to the countries with which mutual assistance is deficient or perfectible.
- Examine whether it would be opportune for Belgian law to enable foreign confiscation decisions to be recognised without any prior conviction.
- Review the legislative framework for extradition outside the EU in order to improve the time taken to process files and to respond to requesting authorities (except when that would be contrary to the fundamental interests of Belgium or in violation of the supranational standards such as conventions for safeguarding personal rights).

TECHNICAL COMPLIANCE ANNEX

1. INTRODUCTION

This annex provides a detailed analysis of Belgium's level of compliance with the *FATF 40 Recommendations*. It does not describe the situation of the country or risks but focuses on analysing the technical criteria for each Recommendation. It should be read in conjunction with the assessment.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to the analysis carried out under the previous assessment of 2005. This report is available at the following address: www.fatf-gafi.org.

2. NATIONAL AML/CFT POLICIES AND COORDINATION

Recommendation 1 – Assessing risks & applying a risk-based approach

a2.1. These requirements were added to the *FATF Recommendations* when they were last revised in 2012 and therefore were not assessed under the previous mutual evaluation of Belgium in 2005.

a2.2. **Criterion 1.1** – Belgium has conducted two national risk analyses. The College for AML Coordination (*Collège de coordination de la lutte contre le blanchiment de capitaux d'origine illicite -- CCLBC*) finalised its analysis in December 2013. The College for Intelligence and Security (*Collège du renseignement et de la sécurité -- CRS*) completed its analysis of terrorist financing risks in February 2014. These documents summarise the knowledge of the different competent authorities regarding ML/TF threats and vulnerabilities that they have developed in recent years.

a2.3. **Criterion 1.2** – In July 2013 (RD of 23 July 2013), Belgium implemented a new organisation of its AML/CFT co-ordination system. The new organisation comprises two entities: (i) the *Ministerial Committee for AML Co-ordination* establishes general AML policy and determines the priorities of the agencies involved in these efforts; and (ii) the *Ministerial Committee for Intelligence and Security* is responsible for determining the general government policy on countering TF and the financing of proliferation of weapons of mass destruction. (The colleges mentioned above fall under these committees.)

a2.4. **Criterion 1.3** – Because Belgium conducted analyses of ML threats and risks in December 2013 and of TF in February 2014, these are relatively up-to-date, although the TF analysis is based on information that sometimes dates back to 2011. Concerning future updates to these analyses, the RD of 23 July 2013 stipulates that national ML analysis should be ‘ongoing and evolving’, which implies that the authorities are required to keep these analyses up-to-date. Although these texts relating to TF risk analysis do not specify the terms and conditions for updating the analysis, the CRS seems to adhere to the same procedures and schedule as the CCLBC.

a2.5. **Criterion 1.4** – Concerning ML, the CCLBC may share the results of its analysis with the institutions and persons subject to the law (namely financial institutions and DNFBPs), the CRS, and with the oversight, supervisory or disciplinary authorities of the concerned institutions and persons. Some of these authorities are already permanent members of the CCLBC. The CRS is responsible for TF analyses. It may provide the results to some of the competent authorities, but there is no mechanism that aims to make the information – notably non-confidential information – available to self-regulatory bodies, financial institutions and designated non-financial businesses or professions.

a2.6. **Criterion 1.5** – Before July 2013 and for a long time prior to that, when the CTIF identified risk and steps needed to be taken to address them, the CTIF suggested necessary legislative changes to the government. Furthermore, it was already the responsibility of the public prosecutor’s office to determine criminal policy in terms of the policy for investigation and prosecution of offences under the authority of the Minister of Justice. The Federal Police then made decisions on the allocation of personnel and material resources consistent with the priorities identified in the National Security Plan, which itself is based on an analysis of criminal threats and risks (including ML).

a2.7. Because the institutionalisation of the risk assessment mechanism is very recent, the response to the risk analysis vis-à-vis the allocation of resources, legislative initiative or other measures has not yet been completely acted upon. However, the institutional framework to do so is in place: Belgium established the Ministerial Committee for AML Co-ordination in 2013 (see C 1.2). This committee must determine and decide – based on proposals from the CCLBC and on risk analyses – the general policy and the measures to take to address the threats and risks identified without making any reference however to resources. The CCLBC is responsible for implementing this general policy. Similarly, in 2013 Belgium gave the Ministerial Committee for Intelligence and Security the task of co-ordinating efforts to combat TF and PF (see C 1.2). This committee is also assisted by the CRS.

NATIONAL AML/CFT POLICIES AND COORDINATION

a2.8. **Criterion 1.6** – According to Art.11§2 of the ‘AML/TF Law’, the entities and persons subject to the law are not subject to identification and verification requirements under certain conditions. These exemptions are not based on an observed low risk of ML/TF resulting from an assessment carried out at the national or European level but on a presumption of low risk. Moreover, they are not limited to a particular type of institution, financial activity or DNFBP. Nor is the application of these exemptions limited to a financial activity carried out on an occasional or very limited basis such that the ML/TF risks are low.

a2.9. **Criterion 1.7** – The AML/TF law (Art. 12) requires financial institutions and DNFBPs to apply enhanced due diligence in high-risk situations and cites in particular those situations identified on the basis of the 2003 FATF Recommendations (contracts negotiated at a distance, politically exposed persons, correspondent banking) – for which it requires the regulated bodies to perform enhanced due diligence. The national ML/TF risk assessments identified a certain number of activities and sectors with high risk for which requirements for enhanced due diligence have not been imposed, although such measures should be applied according the general rule of Art. 12.

a2.10. **Criterion 1.8** – Belgian authorities report that simplified due diligence is authorised and that it may be applied in the situations described in Art.11§1 of the AML/TF law (see C 10.18). However, no risk analysis has been performed at the national or European level that establishes that all of these situations present a lower risk.

a2.11. **Criterion 1.9** – The AML/CFT Law stipulates that supervisors implement effective mechanisms to ensure that the regulated entities and persons comply with the preventive requirements stipulated by the law (Art.39§1). Moreover, obligated entities and persons are required to take ML/TF risks into account in the customer acceptance policies and in implementing AML/CFT measures (see C.1.10). However, the AML/CFT inspection systems for the financial sector and DNFBPs have shortcomings in the area of the risk-based approach (see R 26 and R 28).

a2.12. **Criterion 1.10** – There is no explicit obligation for obligated entities to make a general assessment of ML/TF risks and to keep it up-to-date. This lack of an explicit obligation is not considered to be a deficiency because the AML/CFT Law stipulates that the entities and persons subject to the law are required to implement most of their requirements in accordance with the risk identified: (e.g. updating identification data; Art. 7§3 and 8§2). Furthermore, the obligated institutions and persons are required to define objective risk criteria (e.g. Art.26 Regulations taken for financial institutions; Art. 8 Regulations for diamond industry; Art. 8.1. Institut des Réviseurs d’Entreprises - IRE standards) which form the foundation on which their risk-based approach must be built. up-to-date. They must also take into account risks, in particular when applying CDD measures and customer relations monitoring (Art. 12, 14 and 16 of the AML/CFT Law). This approach implies that they conduct an analysis of risks that may affect them.

A2
a2.13. **Criterion 1.11** – (a) Financial institutions and DNFBPs that are required to define objective risk criteria (see C.1.10) must set out adapted preventive measures (e.g. Art. 26, Regulation for financial institutions; Art. 8 Regulations for diamond traders; Art. 8.1. IRE standards). Moreover, the AML/CFT Law requires that regulated institutions and persons be able to justify to their respective supervisors that the scope of the measures put in place is adequate and appropriate in light of the ML/TF risks when they deviate from the scope of the AML/CFT requirements based on the risk identified (Art. 38§2). For financial institutions, the obligation for approval by senior management of the policies, controls and procedures for managing and mitigating the risks flows from general prudential principles. b) The law stipulates that regulated institutions and persons are required to implement adequate internal audit procedures that specifically take into account the heightened ML/TF risk in order to ensure compliance with the law (Art.16§1). c) The law stipulates that regulated institutions and persons must implement certain requirements in response to any higher risks identified (Art. 12§1).

a2.14. **Criterion 1.12** – The law allows the application of simplified measures only in the cases described in Art.11§1 of the AML/TF Law (see C.10.18) and does not allow financial or non-financial institutions any discretion to apply simplified measures in other situations.

Weighting and conclusion

a2.15. Measures for assessing the risks of the country are in place as are the necessary mechanisms for taking the evolution of these risks into account and for defining the information of interested parties. Additionally, those subject to the AML/CFT law are required to identify their ML/TF risks in order to implement appropriate measures, core requirements of R 1. Nevertheless, the scheme lacks certain elements, and in particular there is no mechanism to ensure the dissemination of the non-confidential results of TF risk assessments to supervisors and regulated entities. Furthermore, the application of exemptions to the AML/CFT scheme or of simplified measures is not justified by assessments of low or lower risk. Finally, efforts are necessary in order for supervisory authorities as a whole to be able to ensure that regulated entities implement their AML/CFT obligations taking risk into account. **Belgium is largely compliant with R 1.**

Recommendation 2 – National co-operation and co-ordination

a2.16. Belgium found to be largely compliant in 2005 with the FATF standard pertaining to national co-operation (formerly R 31) because of the lack of consultation between the CTIF and the FPSs having authority to control professions not subject prudential supervision.

a2.17. **Criterion 2.1** – The principle of a national AML/CFT policy was institutionalised by the two RDs of 23 July 2013. It falls to the Ministerial Committees created to draw up this policy (see C.1.2. and C.1.5); the national risk analysis must be ‘ongoing and evolving’ and must make it possible to adapt the strategies to the phenomena identified. Because this framework is recent, Belgium has not yet defined overall national AML/CFT policy underpinning policies to prevent and combat ML/TF. (Some sectoral policies exist: Until now, the public prosecutor’s office has determined criminal policy consistent with the policy to investigate and prosecute offences [including laundering] under the authority of the Ministry of Justice.)

a2.18. **Criterion 2.2** – Co-ordination mechanisms have been instituted to draw up a national AML policy, and an authority has been designated for this purpose. Such mechanisms also exist for CFT (see C.1.2).

a2.19. **Criterion 2.3** – The mechanisms for co-operation on the drafting of policies as set forth in the RDs of 23 July 2013 are supplemented by measures that organise operational co-ordination. This is notably the case between the CTIF and the other government agencies (including supervisors) and judicial authorities (see R 29). Several MOUs between the CTIF and its partners spell out the terms of information sharing. The CTIF hosts liaison officers from other government entities. Co-ordination methods and processes have also been put in place by the Federal Police (with AGDA) and by the College of Prosecutors-General (network of experts who in particular address matters relating to ML). The FSMA and BNB have adopted a protocol that organises their exchanges of information, including for AML/CFT information.

a2.20. **Criterion 2.4** – The Ministerial Committee for Intelligence and Security is responsible for co-ordinating efforts to combat the financing of PF. The co-ordination procedures described above (see C.2.3) apply in this area, and the same authorities are involved as for TF. However, certain other authorities that are responsible for implementing freezes relating to PF are not involved directly in the activities of the CRS, notably FPS Finance and Treasury Administration.

Weighting and conclusion

a2.21. There is not national (overall) AML/CFT policy that takes into account the recently identified risks, but the basic elements for national co-operation and co-ordination (C.2.1 and C.2.3) are in place for the most part, in light of its development in the near term. **Belgium is largely compliant with R 2.**

Recommendation 33 – Statistics

a2.22. In 2005, Belgium was evaluated as largely compliant with the FATF standard that covers the collection of statistics (formerly R 32). Indeed, some statistical data was missing (with regard to the CTIF and pertaining

A2

to mutual legal assistance and extradition). Although the CTIF now has comprehensive statistics, there is still a lack of information on international co-operation.

a2.23. **Criterion 33.1 -**

- a. The CTIF keeps statistics for its own internal use and for dissemination in its reports. These statistics include the number of STRs received and disseminated. The range of statistics relevant to these statements is broad and helps with the processing, management and monitoring of STRs received. There are also statistics that enable the quantification of the number of court decisions relating to cases submitted by the CTIF to the judicial authorities, in which ML and TF convictions were handed down in connection with one or several predicate offences.
- b. The Federal Police have their own statistical tool that inventories the investigations in progress, notably those relating to ML/TF offences. The College of Prosecutors-General has a database that contains the records from the correctional sections of the 28 public prosecutor's offices at the trial courts (REA/TPI system); it identifies prosecutions relating to ML/TF. This statistical tool is incomplete because it does not include statistical data from all the public prosecutor's offices; it does allow for distinctions between prosecutions linked to terrorism and those relating to TF. Statistics about the number of ML- and TF-related convictions are available, but incomplete because of delays in recording.
- c. Statistical data about seizures and confiscations are available, but the data held by the OCSC are piecemeal (see discussion on effectiveness in conjunction with IO 8, Section 3.5 of the report).
- d. The computer system at the Mutual Criminal Legal Assistance Department can now provide accurate statistical data but only pertaining to requests received since 1 January 2013. Similarly, the CTIF collects quantitative data about the number of information requests received and sent, as well as the breakdown by foreign FIU of information requests received or sent by the CTIF. The police's national general database cannot provide statistics about international co-operation. Nevertheless, the judicial police have data about the joint investigation teams (JITs), for example. The AGDA maintains statistical data about the number of spontaneous reports and requests for assistance it receives and sends.

Weighting and conclusion

a2.24. While the statistics relevant to STRs and investigations are good, those pertaining to prosecutions and convictions for ML and TF are not up-to-date. The data on property seized and confiscated are fragmented and unreliable. Data pertaining to mutual legal assistance are virtually non-existent even though the ML/TF risks in Belgium are often international in nature. **Belgium is partially compliant with R 33.**

A2

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Recommendation 3 – Money laundering offence

a3.1. In 2005 Belgium was evaluated as compliant with the FATF standard that criminalises ML (formerly R 1 and R 2). Since then, the offence has been modified slightly, particularly as regards confiscation.

a3.2. **Criterion 3.1** – The criminalisation of ML (Art. 505 PC) incorporates the material elements which constitute the offence as defined in the Vienna and Palermo Conventions.

a3.3. **Criteria 3.2 and 3.3** – All crimes (*crimes et délits*) under Belgian law may constitute predicate offences. In Belgium, the ML offence covers the laundering of *material benefits* from all the offences included in the FATF definition of *designated categories of offences*.

a3.4. **Criterion 3.4** – The ML offence extends to the material benefits derived directly from the offence, as well as property that indirectly represents the proceeds of crime: the property (defined broadly) and the values that have been substituted for them, as well as income earned on investing these proceeds (Art. 42 – PC).

a3.5. **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 be derived from the official income of the defendant; therefore the illegal origin of proceeds can be deduced from the circumstance by which there is no credible data indicating the origin can be legal (*Cassation*, 17 December 2013).

a3.6. **Criterion 3.6** – The criminalisation of ML extends to acts committed in another country that constitute an offence in that country provided that they also constitute an offence under Belgian law. The commission of ML acts on Belgian soil is sufficient, even if the predicate offence was committed in another country (provided that these acts would have also constituted an offence if they had occurred on Belgian soil).

a3.7. **Criterion 3.7** – Art. 505 al. 2 PC stipulates that the ML offence applies also to the persons who commit the predicate offence (*self-laundering*).

a3.8. **Criterion 3.8** – The principle of freedom of evidence is an overriding principle in Belgian evidentiary law. Under Art. 505 al. 2 PC pertaining to natural persons who knew or should have known about the illegal origin of laundered assets, the intentional element and knowledge of the facts required to prove the ML offence can therefore be inferred from objective, factual circumstances.

a3.9. **Criterion 3.9** – The sanctions applied to natural persons convicted of ML are proportionate and dissuasive. In the scale of sanctions that may be applied to offences in Belgium, the sanction provided for ML is in the higher end of the average range (5 years) and is equivalent to other, comparable financial offences (possession of stolen goods, misappropriation of corporate assets). ML is punishable by 15 days to 5 years in prison and/or a fine of EUR 156 to EUR 600 000 (Art. 505 al. 1 PC¹). Furthermore, confiscation (Art. 43ff. PC) applies to the proceeds of the crime and can be added as an additional sanction, whose purpose is to reinforce the dissuasive nature of the sanctions (see R 4). The court also has the ability in all cases to add additional sanctions such as the withdrawal of certain rights or of the right to hold certain positions or jobs.

1 The indexation system makes it possible to increase the penalty set forth in the law by multiplying it by a legally defined coefficient that is regularly updated to reflect the present value of money. In July 2014 this coefficient was X6.

a3.10. **Criterion 3.10** – According to Art.5 PC, all legal persons are criminally liable for offences that are intrinsically linked to the fulfilment of its corporate purpose or to the defence of its interests or for offences that have been committed on its behalf. In the event that this liability is incurred solely because of the actions of an identified natural person, ‘only the person who committed the most serious offence can be convicted’. Moreover, the PC stipulates that, ‘if the identified natural person committed the offence knowingly and voluntarily, said person may be convicted at the same time as the liable legal person’, which suggests causality between the legal liability of the company and that of the individual. Finally, the criminal liability of legal persons in place since 1999 does not preclude in any way the ability for them to be subject to civil liability.

a3.11. The range of applicable sanctions is broad and the sanctions available seem proportionate and sufficiently dissuasive. The applicable sanctions are: a fine (from EUR 3 000 to EUR 1.2 million), 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. 7a PC). The Law of 1999 stipulates that convictions of legal persons are to be entered in a criminal record kept by the registry of the competent court. These amounts are comparable to the amounts of fines set forth for other financial offences such as corruption and crimes relating to bankruptcy.

a3.12. **Criterion 3.11** – Belgium has appropriate ancillary offences to the ML offence. Facilitating the commission of the offence and conspiracy to commit an offence can be construed as criminal participation or aiding and abetting (Art. 66, 67 and 68 PC). Criminal conspiracy and participation in a criminal organisation that facilitates, in particular, the commission of an offence relating to acts of ML are also punishable. Attempt to commit is criminalised in Art.51 PC.

Weighting and conclusion

a3.13. **Belgium is compliant with R 3.**

Recommendation 4 – Confiscation and provisional measures

a3.14. Belgium has a seizure and confiscation mechanism that was evaluated as largely compliant with the FATF standard in 2005 (formerly R 3). In particular, clarification was expected with regard to the confiscation of assets of equivalent value and was provided in 2007, along with other improvements.

a3.15. **Criterion 4.1** - Article: 42ff.PC establishes a special confiscation regime, namely one that is ancillary to a primary sanction, which applies to all categories of offences, including ML, TF and terrorism. Since 2007, confiscation can be imposed on all perpetrators, co-perpetrators or accomplices of laundering, even if the property does not belong to the convicted person.

a3.16. **Criterion 4.2** – The Law of 19 December 2002 introduced the ability to conduct a specific investigation into the material benefits described in Art. 42, point 3, 43a and 43c PC in order to confiscate them. This measure was strengthened by a recent law (Law of 11 February 2014). Different types of provisional measures to prevent transactions involving property subject to confiscation are available in Belgium. These provisions enable the seizure of objects, instruments and proceeds of the crime, as well as of the material benefits derived directly from offences, property and values that have been substituted for them and income from invested proceeds. Several freezing measures are also available to administrative (including the CTIF) and judicial authorities that aim to place certain assets under control so that subsequent confiscation is possible (also see R 6).

a3.17. **Criterion 4.3** – The rights of bona fide third parties are protected by law.

a3.18. **Criterion 4.4** – The management of material assets seized has been entrusted since 2003 to the OCSC. This entity under the public prosecutor’s office has the primary responsibilities of assisting judicial authorities with seizing material assets and executing decisions and decrees resulting in the confiscation or restitution of material assets.

A3

Weighting and conclusion

a3.19. **Belgium is compliant with R 4.**

Operational and prosecutorial matters

Recommendation 29 – Financial Intelligence Units

a3.20. Belgium was evaluated in 2005 as compliant with the FATF standard pertaining to the authority and powers of the FIU (formerly R 26).

a3.21. **Criterion 29.1** - The Belgian FIU is the *Cellule de Traitement des Informations Financières* (CTIF), which was created by the AML/CFT Law. It is the agency in charge of receiving, analysing and transmitting AML/CFT information and of analysing information received in relation to ML, related predicate offences and TF.

a3.22. **Criterion 29.2** – The CTIF serves as the central agency for the receipt of disclosures filed by reporting entities, including STRs (see R 20 and R 23). In addition to STRs, submitted on the basis of subjective criteria, the CTIF receives and processes other reports under the AML/CFT Law based on objective criteria (notably reports received for non-compliance with the prohibition of cash payments for real estate assets, Art. 20 – AML/TF Law; reports on cross-border transportation of cash; reports filed by casinos).

a3.23. **Criterion 29.3** – Under the AML/CFT Law, the CTIF can obtain any additional information of a financial, administrative or legal nature which it deems useful to carrying out its mission. When a matter is brought properly before it (i.e. under the terms of Art. 22 of the AML/CFT Law notably), the CTIF can question and obtain information from any reporting entity (without restriction), from the chairman of the bar association (under certain conditions, see R 23), from trustees in bankruptcy and interim administrators, from judicial authorities (provided that the filing is authorised by the public prosecutor or the Federal Prosecutor), from the administrative agencies of the national government and from the police. The collection of information from public authorities is facilitated by the secondment of liaison officers to the CTIF. The CTIF can also share information with the Anti-Fraud Co-ordination Service (with regard to combatting tax fraud) and with the BNB and the FSMA. In order to perform its functions, the CTIF has access to the financial and other information (from private and public sources) necessary to carry out its activities.

a3.24. **Criterion 29.4** – The Analysis Department of the CTIF conducts operational analysis using the information it receives and collects. Analytical work is explained in a guide given to each analyst. Furthermore, in 2009 the CTIF created a strategic analysis department tasked with conducting proactive research on trends in ML and TF.

a3.25. **Criterion 29.5** – Whenever analysis reveals reliable indicators of ML, TF or PF, the public prosecutor or federal prosecutor is notified. The law also provides for the dissemination of information by the CTIF to other competent authorities, both spontaneously and upon request (notably OLAF and entities with oversight and regulatory authority over institutions and professions subject to the AML/CFT Law under certain conditions). There are no secure, protected channels for this communication. Notifications of acts of laundering that the CTIF submits to the public prosecutor's office are hand delivered by the CTIF (in Brussels) or sent by registered mail (and, in an emergency, by fax).

a3.26. **Criterion 29.6** - A comprehensive legislative mechanism was put in place to ensure the confidentiality of information held by the CTIF and of its dissemination in accordance with the provisions of the law. The personnel of the CTIF are held to a strict obligation of confidentiality which bars any external disclosure acknowledging the existence and content of the individual cases handled. *Memoranda* and a *code of ethics* establish several aspects pertaining to the protection of sensitive and confidential information and fundamental principles such as strict professional secrecy, loyalty, compliance and security. Finally, queries in internal and external databases are limited strictly to the purposes defined in the AML/TF law.

A3

a3.27. **Criterion 29.7** – The CTIF is an administrative authority established as a legal entity under the AML/CFT Law (Art. 22). The following elements ensure its independence and operational autonomy:

1. The CTIF has extensive autonomy both in the fulfilment of its mission (decisions taken, external collaboration, internal organisation, etc.) and in administrative matters (including its budget). The details pertaining to the composition, organisation, function and independence of the CTIF are determined by royal decree (RD of 11 June 1993).
2. The CTIF has adequate powers which enable it to negotiate agreements or determine in total independence to collaborate with other relevant national authorities or with its foreign counterparts via MOU (Art. 22, AML/CFT Law,).
3. The CTIF is subject to joint administrative oversight by the Ministers of Justice and Finance which have no control over the decision-making power of the CTIF: they cannot give it instructions, injunctions or orders, notably with regard to the decision of whether to submit a case to the public prosecutor's office.
4. The CTIF is able to obtain and deploy the resources needed to carry out its functions. Its budget is not funded by the national government, but rather is made up of contributions paid annually by the institutions and professions subject to the AML/CFT Law.

a3.28. **Criterion 29.8 – This criterion is not applicable.** The CTIF is one of the founding members of the Egmont Group.

Weighting and conclusion

a3.29. **Belgium is compliant with R 29.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

a3.30. In 2005 Belgium was evaluated as compliant with the FATF standard pertaining to the responsibilities of law enforcement authorities (former R 27).

a3.31. **Criterion 30.1** – In Belgium several law enforcement authorities are able to conduct investigations into ML, TF or predicate offences for ML. The Ministry of Justice is competent in judicial investigations carried out under the orders of local investigative authorities and of the federal prosecutor. The allocation of ML cases to court districts is based on different criteria (geography, international dimension, links to organised crime, etc. and consistent with the CCP). The prosecutor may decide to bring a matter before an investigating judge, especially for complex cases. The federal prosecutor's office initiates prosecution for a set list of offences (including TF) and works to facilitate international co-operation.

a3.32. There are two different levels of police (local and federal) that function in an integrated and complementary manner. The national judicial police have responsibility across the entire country for carrying out the specialised and supra-local missions associated with criminal policing and for providing support to local and other police authorities. It reports to the Ministers of Interior and Justice who may give orders, instructions and directives necessary to the performance of its judicial police duties. Within the national judicial police, the Directorate for Combatting Economic and Financial Crime (DJF) and the Directorate for Combatting Crimes against Persons (DJP), as well as the decentralised directorates (called PJFs) which are responsible for, in particular, pursuing ML/TF matters. Within the DJF, the Central Office for Combatting Organised Financial Crime (OCDEFO) is specifically responsible for combatting ML. Within the DJP, the Terrorism and Sects Department is responsible for combatting TF.

a3.33. **Criterion 30.2** – The police promote a cross-cutting approach to AML, notably within the OCDEFO. All the departments in charge of fighting priority criminal phenomena must be able to conduct asset investigations or receive support from units specialised in this type of investigation. Within the Brussels

PJF, there is a terrorism investigation department that takes on both distinct TF investigations as well as the financial aspects of investigations relating to a terrorism case managed by the department. One or several investigating judges specialised in terrorism matters are designated within the circuit of each court of appeals.

a3.34. **Criterion 30.3** – The criminal prosecution authorities have the power to identify, trace and initiate procedures to seize property that may be proceeds of crime (see R 4). Asset tracing investigations may be ordered by the public prosecutor’s office or the investigating judge in order to assess the property to be seized. In addition, the public prosecutor’s office can ask the trial judge – after conviction – to order a specific investigation into material benefits. A recent law strengthens the role of the OCSC in asset investigations (see R 4). AGDA is empowered to detain some funds in relation to controlling the cross-border transportation of money (see R 32).

a3.35. **Criterion 30.4** – Authorities which are authorised to conduct financial investigations of predicate offences are law enforcement authorities as described for C.30.1. In addition, the Special Tax Inspectorate (ISI) within FPS Finance is responsible for combatting certain financial offences, including serious tax fraud, financial fraud and misappropriation of corporate assets. AGDA also assists with efforts to combat fraud, organised crime and terrorism and with the implementation of requirements relating to controlling the cross-border transportation of funds (see R 32).

a3.36. **Criterion 30.5** – In Belgium, the investigation and prosecution of ML/TF resulting from or relating to a corruption offence generally fall under the purview of federal authorities.

Weighting and conclusion

a3.37. **Belgium is compliant with R 30.**

Recommendation 31 – Powers of criminal prosecution and investigative authorities

a3.38. In 2005, Belgium was evaluated as compliant with the FATF standard pertaining to the powers of criminal prosecution and investigative authorities (formerly R 28). This Recommendation was expanded in 2012.

a3.39. **Criterion 31.1** – During investigations of ML, predicate offences and TF, the police employ traditional investigative methods (use of open source information, seizures, taking statements, searches, etc.) as provided for in the CCP. Financial institutions are required to respond to requests from the public prosecutor and cannot refuse a search or seizure of documents relating to their customers (Art. 46d CCP). These measures do not apply to persons held to professional secrecy sanctioned by Art.458 PC (including attorneys, notaries public, accountants and tax advisers). In this case, the requested items may be handed over voluntarily or forcibly upon obtainment of a targeted search warrant by the investigating judge who has the authority to decide which evidence is protected by professional secrecy and thus cannot be seized.

a3.40. Judicial police officers can search private premises (residence or business location). Searches are only possible if judicial authorities have reliable evidence that an offence has been committed. In the framework of judicial investigation, it is possible to take statements from suspects and witnesses (Art. 47a CCP). Statements cannot be taken from persons bound to professional secrecy, but these individuals can testify in a legal court. Finally, the public prosecutor or the investigating judge can seize anything that may serve to reveal the truth. All evidence must be obtained fairly and legally. The ISI uses the prerogatives of the Income Tax Code and the VAT Code to conduct its investigations, notably with regard to tax fraud, and to gain access to any document or information it deems necessary, including access to the business or other premises and the production of documents held by financial institutions under certain conditions.

a3.41. **Criterion 31.2** – The judicial police can use the special investigation techniques described in Art. 40a (deferred actions, to include controlled deliveries), 47b to 47j (undercover operations, surveillance, use of informants) and 90b CCP (interception of communications and telecommunications), under the supervision of the public prosecutor’s office and in the framework of an investigation or inquiry. The police may use techniques to access computer systems under certain conditions (Art. 88b CCP). The Law of 6 January 2003

A3

on special investigation techniques and certain other investigative methods governs the interception of mail, discreet visual checks and delayed actions. The Law of 4 February 2010 on data collection methods used by intelligence and security agencies confers on those agencies other investigation techniques useful for AML/CFT. The ISI can gain access to the computer systems of the natural or legal persons it audits.

a3.42. **Criterion 31.3** – The public prosecutor’s office can access banking information pertaining to natural or legal persons with a substantiated written order (Art. 46c Paragraph 3 CCP). The authorities indicate that the time necessary for such a decision to be taken depends on the needs of the investigation (emergency or normal procedure) and that the turnaround time for accessing the information depends on the time it takes financial institutions to process the request. Nothing in the law blocks the obtaining of information in a timely manner. This information is obtained without giving prior notice to the owner [of the assets] (see Art.46c Line 3 CCP). Pursuant to the Law of 14 April 2011, the Belgian Tax Agency and the police have access to a national database maintained by the BNB to which all banking, currency exchange, credit and savings institutions must submit the identities of their customers and the account and contract numbers of said customers.

a3.43. **Criterion 31.4** – The police can access the information held by the CTIF only in cases where this information has been previously submitted to the public prosecutor’s office, notably via liaison officers from the Federal Police who have been seconded to the CTIF. Nevertheless, it is possible to obtain a legal exemption from this general rule. The AML/CFT Law (Art. 33) stipulates that the police can spontaneously provide information regarding investigations underway to the CTIF. If the CTIF has relevant information for the investigators and if there is reliable evidence of ML or TF as defined by law (which, according to the authorities, is the case when the investigation concerns one of the predicate offences described in the law), the CTIF submits the information in its possession to the judicial authorities and will notify the investigators of this submission.

a3.44. Thus the law enforcement authorities (public prosecutor’s office, investigating judges and police) can have access to relevant information held by the FIU. For the public prosecutor’s offices, it should also be added that the CTIF makes a secure internet connexion available to magistrates designated by the country’s 28 public prosecutor’s offices and a database of files submitted by the CTIF since 1993. Finally, since the Law of 11 February 2014, the OCSC has very broad powers to obtain information from the CTIF.

Weighting and conclusion

a3.45. **Belgium is compliant with R 31.**

Recommendation 32 – Cash couriers

a3.46. In 2005 Belgium was evaluated as non-compliant with the FATF standard pertaining to the cross-border transport of currency and other financial instruments (formerly SR] IX) because it did not have a system to control cash movements at its borders. A control mechanism for cross-border transportation of currency and other financial instruments has been in place since 2007; it is based on two levels of regulation: European and national (RD of 2006 then 2014).

a3.47. **Criterion 32.1** – Regulation No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the European Community applies to the movement of cash into or out of states outside the EU. The RD of 26 January 2014 containing certain measures to control the cross-border transportation of cash establishes the control of extra-Community currency movements using a *declaration* system and to control intra-Community currency movements using an on-request *disclosure* system. Therefore Belgium has set up two models to control the movement of funds based on the destination or source country of the cash and bearer negotiable instruments (BNIs).²

2 The definition of BNI which appears in Art. 3 of the RD of 26 January 2014 and in Art. 2 line 2 of Reg.1889/2005, complies with the one set forth in the Glossary of the *FATF Recommendations*.

a3.48. The European regulation (which applies only to natural persons), does not cover the physical transportation of cash or BNIs through container cargo or the shipment of cash or BNIs through mail. This type of transportation (through cargo or mail, including on behalf of a legal person) is only mentioned in the RD of 26 January 2014 with regard to the intra-Community transportation of cash and BNIs. For extra-Community transportation, a customs declaration prepared under the normal procedure must still be presented with the correct customs codes and the value of the cash.

a3.49. **Criterion 32.2** – Belgium has a declaration system for the cross-border transportation (incoming and outgoing) of cash or BNIs between Belgium and third countries outside the EU above a threshold of EUR 10 000 (or equivalent value, Art.3 of Regulation 1889/2005). The declaration must be filed in writing or in electronic form with the competent authority (Art. 2 of the RD of 26 January 2014).

a3.50. **Criterion 32.3** – Art.4 of the RD of 26 January 2014 establishes the control of currency transportation between Belgium and an EU member country and establishes a communication system (in this case the cash courier must declare, only upon request by the competent authority, if transporting cash in the amount of EUR 10 000 or more).

a3.51. **Criterion 32.4** – In application of the RD of 26 January 2014, AGDA officers and police officers can perform *de facto* inspections of natural persons, their means of transportation and their luggage. In practice, detection is carried out by AGDA and subsequent investigations are conducted by the Federal Police. AGDA officers can require the presentation of documents establishing the identity of persons involved and obtain information (via a standardised declaration form) on the origins of the funds, the owner and recipient of the funds and on the use for which they are intended.

a3.52. **Criterion 32.5** – Under Regulation 1889/2005, in the event of an incorrect or incomplete declaration, the declaration obligation has not been met (Art. 3). Under the RD of 26 January 2014, any attempt to violate the obligation to declare extra-Community currency movements (in application of Regulation 1889/2005) is punished with a fine of EUR 125 to EUR 1 250 (doubled for a repeat offence). This sanction is imposed when it appears that the failure to declare is the result of a mere oversight on the part of a passenger who forgot to declare or who was apparently unaware of the law. The Belgian authorities explained that the intention of the fine in cases of a failure to declare or false declaration (when there is no other indicator of the violation of another law, particularly in relation to ML/TF) justifies the amount. They note that a preliminary ruling about the amount of these fines is pending before the CJEU. The authorities indicated that, as soon as customs authorities suspect that the funds are from of illegal origin, the transportation of funds is a distinct act and may be punishable following an investigation (the sanctions being in accordance with the related offence). With regard to the disclosure of intra-Community currency movements, Art.6 stipulates also that in the case of incorrect or incomplete information, it is considered that the declaration obligation was not met. Moreover, any violation of this obligation is punished by imprisonment of eight days to five years and by a fine of EUR 25 to EUR 25 000. In the framework of declaration and disclosure, if there is evidence that leads to suspicion that the cash comes from illegal activity or is meant to fund such activity, the money is detained by the competent authority (see C.32.8).

a3.53. **Criterion 32.6** –AGDA records and analyses declarations and disclosures of currency movements and makes them available to the CTIF which is authorised to receive such information. Under the AML/CFT Law, the declarations and disclosures received in application of the aforementioned RD are considered in the same way as STRs, just as the declarations received from other persons and institutions subject to the law. The authorities indicated that the data from extra-Community currency declarations are submitted each week to the CTIF. Disclosures obtained upon request (intra-Community transfers) are also submitted to the CTIF (via the Central Office for Information Management and Risk Analysis). The reports on all violations of the declaration obligation are sent to the public prosecutor's office, and a copy goes to the CTIF.

a3.54. **Criterion 32.7** – Co-operation between AGDA and the police is based on a framework agreement that organises their collaboration, information exchanges and joint risk and fraud analysis, notably in cases of joint inspections. The Law of 18 March 2014 on the management of police information now authorises the two-way communication of data and other information to enable the other authorities to fulfil their legal responsibilities. The terms of this sharing are set forth in an MOU approved by the ministers in question.

A3

LEGAL SYSTEM AND OPERATIONAL ISSUES

a3.55. **Criterion 32.8** – In the event of non-compliance with the obligation to disclose intra-Community currency movements or if the declaration obligation was met, but there is evidence to suggest that the cash is derived from illegal activity or is intended to fund such activities, the money is detained by the competent authority (Art.8 – RD 2014). The money cannot be detained for more than 14 days. Detention is an administrative measure whose goal is to give the competent judicial authorities the time to conduct a focused investigation. During the aforementioned 14-day period, the public prosecutor’s office can decide (i) to release the cash; in this case, the cash is made available to the carrier, who can come retrieve it; or (ii) to seize (through legal action) the cash; in this case, the cash shall be deposited with the registry or paid into the OCSC account (see C.4.2). This 14-day period is not enough to conduct an investigation into the origin of the funds, but it can be followed by a legal seizure of the funds which enables the money to be restrained for a reasonable period so that it can be determined whether proof of ML/TF is likely to be found. In the event of non-compliance with the declaration obligation stipulated in Regulation 1889/2005, the funds may be restrained by administrative or judicial decision.

a3.56. **Criterion 32.9** – Declarations and disclosures about cash transfers in amounts equal to or greater than EUR 10 000 are recorded in the AGDA database (see C.32.6, Art. 9 – RD 2014). The CTIF has access to it, which enables sharing with its foreign counterparts. Moreover, Belgium is party to the Convention of 18 December 1997 on Mutual Assistance and Co-operation between Customs Administrations (*Naples II*). Finally, it also enforces Regulation No. 515/97 which calls for the implementation of a rapid and effective system to share information between customs authorities. A customs information system at the Community level contains information regarding undeclared currency movements.

a3.57. **Criterion 32.10** – The information collected from declarations of extra-Community cross-border movements of funds is subject to professional secrecy. Information is disclosed or disseminated in strict compliance with data protection provisions. Point 1 in the Preamble of Regulation 1889/2005 reiterates that the European Community endeavours to create a space without internal borders in which the free movement of goods, persons, services and capital is ensured.

a3.58. **Criterion 32.11** – In the event of non-compliance with the declaration obligation or if the obligation to declare was met, but there is evidence to suggest that the cash is derived from illegal activity or is intended to fund such activities, the money is detained by the competent authority (Art. C.32.8). If this suspicion is confirmed, seizure and confiscation measures may be decided upon 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

a3.59. **Belgium is compliant with R 32.**

A3

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Recommendation 5 – Terrorist financing offence

a4.1. In 2005 Belgium was judged to be compliant with the FATF standard on the criminalisation of TF (formerly SR II). Belgian law has not undergone any substantial modifications since.

a4.2. **Criterion 5.1** – TF is addressed in Art. 140 Para. 1 and 141 PC (unchanged since their introduction in 2004). Belgian positive law does not, as a general rule, regard TF as a principal offence. Art.140 considers TF to be an instance of participating in an activity by a terrorist group, defined as providing information or material resources to the terrorist group, or as any form of financing of an activity by a terrorist group, with the knowledge that this contribution will assist the terrorist group in committing a crime (*crime ou délit*) (in Belgium or somewhere else). As for a terrorist group, it is defined (Art. 139 PC) as a structured association of more than two people established over time, and which acts in a unified way with the intention of committing terrorist acts as defined in Art.137 PC which contains the offences mentioned in Art. 2(1) b) of the UN Convention for the Suppression of the Financing of Terrorism (TF Convention).

a4.3. Art.141 PC criminalises any person who, outside of those cases spelled out in Art.140 PC, provides material resources, including financial assistance, with the intention of committing a terrorist act as described in Art.137 PC.

a4.4. **Criterion 5.2** – The intent and material elements of TF offences are largely addressed:

- *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 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. The law does not introduce any restriction, namely funds do not have to be provided directly to constitute an offence.
- *Providing or collecting funds used with the intention of committing one or several terrorist acts*. Art.140 PC stipulates that the criminalised act must contribute to the commission of a crime (*crime ou délit*) by the 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)). Collecting or providing funds to one or two terrorists without a connection to any specific terrorist act(s) is not criminalised in Belgium. However, the authorities indicate that measures in the PC make it possible to prosecute and punish both the act of financing a terrorist group (Art. 140 Para. 1 PC) and the act of financing a terrorist acting alone (Art. 141 PC). Providing funds to an individual, although not specifically stipulated, would fall under the category of acts not covered by Art.140 but covered by Art.141. Jurisprudence confirms that assistance to a terrorist group in the absence of a link to a specific terrorist act is punishable, as long as the person who provides this assistance “has knowledge of the terrorist aspiration of the group” (Brussels court 25/06/2012, Brussels Court of appeal 1/12/2010).

a4.5. **Criterion 5.3** – 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.

TERRORIST FINANCING AND FINANCING OF PROLIFERATION

a4.6. **Criterion 5.4** – The law does not require *in theory* that the funds be used to commit the TF offence. 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 inducted under Criterion 5.2, Art.140 does not require *in theory* that the funds 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 PC make it possible to go after persons who provide to the terrorist organisation or to a terrorist acting alone, 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 overturned) by jurisprudence concerning assistance to terrorists not acting within a terrorist group.

a4.7. **Criterion 5.5** – Belgian law recognises the principle of freedom 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. Thus it is possible for the intent of the TF offence to be inferred from objective factual circumstances.

a4.8. **Criterion 5.6** – The sanctions 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 sanction immediately below, in compliance with Art. 80 and 81 PC. While the imprisonment fines seem to be proportionate and dissuasive, the pecuniary penalties which are capped at EUR 30 000 do not seem dissuasive.

a4.9. **Criterion 5.7** – The criminal liability of legal persons called for in Art.5 PC applies to the TF offence. 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. 7a 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 sanctions seems relatively broad and the sanctions available seem sufficiently dissuasive.

a4.10. **Criterion 5.8** – As a separate offence, TF is subject to the rules in the PC that criminalise attempts (article 51). The acts of complicity listed in Art.2(5) of the TF Convention are also covered by Belgian law (Art. 66 and 67 PC on co-accomplices).

a4.11. **Criterion 5.9** – In Belgium, TF offences constitute ML predicate offences because Art.505 PC refers to the material benefits derived from any offence.

a4.12. **Criterion 5.10** – 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. 10b and 12 CCP).

A4

Weighting and conclusion

a4.13. Collecting or providing funds to one or two people does not seem to be covered by the TF offence if the connection to a specific terrorist offence cannot be established (C.5.2). Furthermore, the maximum pecuniary penalty of EUR 30 000 does not seem dissuasive (C.5.6). **Belgium is largely compliant with R 5.**

¹ Legal indexed value (see note at R.3).

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

a4.14. In 2005 Belgium was deemed to be partially compliant with FATF standard pertaining to targeted financial sanctions related to terrorism (formerly SR III). Indeed, the definitions of funds or other property to be frozen or confiscated that appear in the European regulations (which are self-executing in Belgium) did not cover all the definitions set forth by the Security Council or FATF. Moreover, pursuant to UNSCR 1373(2001), Belgium did not have the power to freeze funds or other property belonging to an entity or person whose entry on the list created by Regulation 2580/2001 had not been decided at the EU level or when the terrorists in question were citizens of the EU (MER 2005, Para.161 to 197). Since then, the last two points were resolved by the RD of 26 December 2006 (confirmed by the Law of 25 April 2007). UNSCR 1267, split in 2011, is now covered by two European regulations: Regulation 881/2002 on Al-Qaida and Regulation 753/2011 on Afghanistan.

a4.15. **Criterion 6.1 in relation to designations pursuant to UNSCR 1267 (1988 and 1989).**

- a. With regard to authorities that are competent to propose persons for designation to the UN Committees, all the agencies represented in the Ministerial Committee for Intelligence and Security have the ability to propose the examination of a designation or de-listing request through the Ministerial Committee for Intelligence and Security, notably on the basis of assessments by OCAM. The final decision is taken at the political level (Council of Ministers) and all communication with the Security Council is conducted through the permanent mission of Belgium to the UN.
- b. All the agencies represented in the Ministerial Committee for Intelligence and Security can identify targets for designation and propose them for examination by the CRS based on their respective competencies and on the rules that govern each agency (e.g. OCAM is competent for acts that may threaten Belgian interests). Several OCAM confidential circulars organise the co-ordination and exchange of information between the relevant competent authorities. It has not been proved that the UNSCR 1373 criteria are followed in all cases.
- c. The standard of proof by which the competent Belgian authorities decide on designation are not known. However, proposals for designation in Belgium are not conditional upon the existence of a criminal proceeding, in keeping with the standard.
- d. 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 Committee or 1988 Committee or the revised rules concerning the reasons for listing, statement of case, etc. Thus the matter is not relevant.
- e. In 2003, based on information conveyed by the Belgian government, the names of two natural persons were added to the lists in annex of the Security Council Resolution (23 January 2003; see MER 2005, Para. 166-167). As the Belgian government has not submitted any proposal for designation since 2002, the level of detail in the proposals is not relevant.

a4.16. **Criterion 6.2 in relation to designations pursuant to UNSCR 1373** (measures at the European level and at the national level are applicable).

- a. At the European level, the EU Council is responsible for proposing the designation of persons or entities (Regulation 2580/2001 and Common Position 2001/931/CFSP). At the national level, the Ministerial Committee for Intelligence and Security is responsible for proposing freeze measures to the Council of Ministers (RD of 28 December 2006). The proposals are submitted to the Council via the permanent mission of Belgium to the UN.

A4

TERRORIST FINANCING AND FINANCING OF PROLIFERATION

- b. The mechanisms described in conjunction with Criterion 6.1(b) also apply to designations relating to UNSCR 1373.
- c. Concerning requests received, the verification of their reasonable basis is handled at the European level by the 'Common Position 2001/931/CFSP on the application of specific measures to combat terrorism' Group (CP 931 Working Party) at the EU Council which examines and evaluates the information to determine whether it meets the criteria set forth in UNSCR 1373.² At the national level, the RD does not make explicit arrangements for the verification of designation requests received, but the Belgian authorities indicate that the requests can be submitted to FPS Foreign Affairs which will send it to the Ministerial Committee for Intelligence and Security (for application of the procedure set forth in Art.3 of the RD of 26 December 2006).
- d. The CP 931 Working Party assesses whether the request is sufficiently substantiated, namely that it is founded on accurate information that establishes that the person or entity meets the designation criteria set forth in Art.1 Para. 2 and 4 of the Common Position 2001/931/CFSP and takes a decision based on reliable and credible evidence without it being conditional on the existence of an investigation or conviction (therefore based on 'reasonable grounds'). At the national level, no rule addresses the standard of proof.
- e. At the European level, there is no formal mechanism that allows for asking non-EU member countries to give effect to the EU list. In practice, some countries (notably those in the process of becoming EU members) are invited to abide by all new CFSP decisions. It is the President of the Council (the Member State that chairs most of the meetings of the Council, including those of the CP 931 Working Party) that contacts the country through the Secretariat of the Council. All designations must be sufficiently substantiated to identify the person to be designated and exclude those having similar or similar-sounding names (Art. 1(5), 2001/931/CFSP). At the national level, there is no formalised procedure under which Belgium could ask another country, including the EU countries, to give effect to freezing measures undertaken in Belgium.

a4.17. Criterion 6.3:

- a. The competent authorities have powers and mechanisms enabling them to identify persons or entities that might meet the criteria for designation. At the national level, the Law of 10 July 2006 relating to threat analysis stipulates that OCAM support services are required (subject to criminal sanctions) to convey to it, at their own initiative or upon request, all pertinent information (and must also assign experts to it). At the European level, all the EU Member States are required to share with one another all the pertinent information in their possession in application of the European regulation on the freezing of assets. They must work together by mutual agreement, through police and legal co-operation mechanisms in criminal matters, to achieve the most extensive level of assistance possible to prevent and combat terrorist acts.³
- b. The designations must take place 'without prior notice' ('ex parte') being given to the person or entity identified⁴. The authorities indicate that the designation that was executed in 2002

2 All the Council CP working parties are comprised of representatives of the governments of Member Countries. The criteria set forth in Common Position 2001/931/CFSP are compliant with those stipulated in UNSCR 1373.

3 Reg. 881/2002 Art. 8; Reg. 754/2011, Art. 9; 2580/2001, Art. 8; and CP 2001/931/CFSP, Art. 4.

4 Reg.1286/2009 Para. 5 of the Preamble and Art. 7a(1).

occurred without prior notice. The Court of Justice of the EU confirmed the exception to the general rule of prior notice of decisions so as to avoid compromising the effectiveness of the freezing measure.

a4.18. **Criterion 6.4** – Targeted financial sanctions are not implemented ‘*without delay*’, which is not compliant with UNSCR 1988 and 1989. A significant delay between the date of designation by the UN and the date of its transposition into European law⁵ arises systematically because of the time needed for consultation between the various competent agencies at the European level and for the translation of the designation into all the EU languages. In 2013, these delays in transposition ranged from 7 to 29 days for the transposition of UNSCR 1989 and from 7 days to 3.5 months for the re-transcription into European law of UNSCR 1988.⁶ A new designation is considered urgent and will therefore be processed faster, while other changes (e.g. de-listing) are considered less urgent and can thus be transposed less quickly. The national freezing measures do not contain any explicit obligation to implement the freeze ‘*without delay*’ and have never been used to compensate for delays incurred at the European level. Conversely, targeted financial sanctions, in application of UNSCR 1373, are implemented by Council regulations (taken in application of Regulation 2580/2001) that are implemented immediately and directly in Belgian law. As a result, these sanctions are implemented ‘*without delay*’. Similarly, freezing measures decided at the national level are to be implemented immediately from the day they are published in the Belgian Official Journal.

a4.19. **Criterion 6.5** – Belgium has the following powers and mechanisms to ensure the implementation of targeted financial sanctions:

- a. Pursuant to UNSCR 1988 and 1989, European regulations establish the obligation to freeze all the funds and economic resources belonging to a person or entity designated on the European list.⁷ It is apparent, however, that because of significant delays in the transposition of UN designations (see C.6.4), freezes are not implemented ‘*without delay*’, and this delay can result in de facto prior notice to the persons or entities in question. For designations under UNSCR 1373, it should be noted that the regulations are self-executing in all Member States and that no prior notice is to be given to the designated persons or entities.⁸ EU nationals are not subject to the freezing measures set forth in Regulation 2580/2001. They are only subject to police and legal co-operation measures in criminal matters.⁹ Art.75 of the Treaty of Lisbon (2007) allows the freezing of assets of designated EU nationals, but the EU has not yet implemented this provision. To address this shortcoming, at the national level in Belgium, Art.2 of the RD of 28 December 2006 calls for the freezing of funds and economic resources owned by persons and entities targeted by the European regulation (including the EU nationals who are mentioned in it) and Art.3 applies to persons who are not targeted by the European mechanisms but would nevertheless be included in a list established by the Ministerial Committee for Intelligence and Security (at this time there no names on this list). Thus Belgium has implemented both sections of the second recommendation made in the

5 Regulations 881/2002 for designation pursuant to UNSCR 1988 and 753/2011 pursuant to UNSCR 1989.

6 During the third cycle of mutual evaluations, these delays ranged from 10 to 60 days.

7 Regulations 881/2002 Art. 2 (1), 1286/2009, Art. 1 (2), 753/2011, Art. 3, and 754/2011, Art. 1.

8 Reg.2580/2001, Art. 2 (1) (a).

9 EU nationals are persons whose origins, primary activities and objectives are in the EU. Art. 4 of CP 2001/931/CFSP and the footnote on page 1 of the Annex.

TERRORIST FINANCING AND FINANCING OF PROLIFERATION

2005 report. Persons who do not abide by the freezing measures set forth in the European regulations are subject to sanctions at the Belgian level.¹⁰

- b.** Pursuant to UNSCR 1988 and 1989, the freezing obligation extends to all the funds or other assets defined in R 6, namely funds owned by designated persons (natural or legal) as well as funds controlled by them or by persons acting on their behalf or on their orders. These aspects are covered by the notion of ‘control’ in Regulations 881/2002 Art. (2), and 753/2011 Art. 3. With regard to UNSCR 1373, the freezing obligation under Regulation 2580/2001, Art. 2(1)(b) and under the RD of 28 December 2006 is not extensive enough.
- c.** At the European level and in compliance with the UNSCR, the regulations prohibit EU nationals and all other persons or entities present in the EU from making funds or other economic resources available to designated persons or entities.¹¹ At the national level, the RD of 28 December 2006 prohibits making funds or economic resources available to persons or entities listed at the European level or in Belgium, in compliance with the obligations of R 6.
- d.** Designation decided at the European level are published in the Official Journal of the EU. No other communication mechanism (of a more proactive nature) is in place (such as sending automatic notifications to financial institutions and non-financial professions). At the national level, the Belgian Federation for the Financial Sector (Febelfin) sends circulars to its members whenever a new embargo is announced (see <https://www.febelfin.be/fr/embargos>), a list that is referenced in a 2011 CBFA circular.¹² Moreover, FPS Finance and FPS Foreign Affairs dedicate a page on their web sites to the topic of financial embargos. On 18 May 2009, FPS Finance published in the Official Journal a notice to affected persons to remind them of their obligations; this notice was reprinted in a message from the CBFA to its members in July 2009. The web site of the CTIF has a page dedicated to the topic of freezes and addresses the matter of suspicious activity reports related to the application of measures to freeze terrorist assets in its Guidelines. Finally, certain non-financial professional associations tell their members about changes made to the lists.
- e.** The natural and legal persons targeted by the European regulations must immediately provide all information that can foster compliance with relevant regulations to the competent authorities of the Member States in which they reside or are present, as well as to the Commission, either directly or through these competent authorities.¹³ The RD of 28 December 2006 establishes an equivalent obligation, namely to submit this information to FPS Finance, Treasury Administration (Art. 8).
- f.** The rights of bona fide third parties are protected at the European and Belgian levels.¹⁴

a4.20. **Criterion 6.6** – Procedures published in the EU and Belgian Official Journals organise the de-listing and unfreezing of funds of persons and entities who no longer meet the criteria for designation.

A4

¹⁰ Regulations 753/2011 Art. 12, 881/2002 Art. 10, 2580/2001 Art. 9, and Law of 11 May 1995 Art. 4 (see MER 2005 Para. 189).

¹¹ Regulations 881/2002 Art. 2(2), 753/2011 Art. 4, and 2580 Art. 2(1).

¹² PF, April 2010, amended in March 2011.

¹³ Regulations 881/2002, Art. 5.1 and 2580/2001, Art. 4.

¹⁴ Regulations 881/2002 Art. 6; 753/2011 Art. 7; 2580/2001 Art. 4; and RD of 28 December 2006, Art. 8.

TERRORIST FINANCING AND FINANCING OF PROLIFERATION

- a. De-listing requests are co-ordinated by the FPS Foreign Affairs and its representative at the UN or via the European Commission.
- b. Pursuant to UNSCR 1373, the Council revises the list at regular intervals (CFSP Art. 6); modifications to the list under Regulation 2580/2001 are self-executing. At the national level, Art.5 of the RD of 28 December 2006 establishes a procedure for requesting removal from the Belgian list. Each request for review must be submitted to the Minister of Finance, who forwards the request without delay to the Ministerial Committee for Intelligence and Security for examination within 30 days. During examination, the Ministerial Committee for Intelligence and Security can ask OCAM to update its assessment. The ministerial committee then sends a proposal to de-list or to maintain a name or to add information for approval by the Council of Ministers.
- c. Pursuant to UNSCR 1373, it is possible to review a designation decision before a court or an independent competent authority in application of Art.263 line 4 of the Treaty on the Functioning of the EU. At the national level, ordinary law applies: the designation decision is an administrative decision that can be challenged before Belgian courts.
- d. and e. For designations pursuant to UNSCR 1988 and 1989, designated persons and entities are notified of their designation and the reasons, as well as its legal consequences; they have the right to request a review of the designation in court. At the European level, there are procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the Council of the EU. Thus this review can be brought before the UN Ombudsman & Mediation Service for the examination of de-listing requests, in compliance with UNSCR 1988, 1989 and 2083, or, where applicable, before the focal point created by UNSCR 1730 pursuant to UNSCR 1988. Belgium can also submit de-listing requests to UN entities.
- f. The procedures described in sub-criteria (a) to (e) apply to the unfreezing of funds or other assets of persons or entities whose name is the same as or similar to that of designated persons or entities who are inadvertently affected by a freeze mechanism. The Belgian authorities indicate that following the identification procedure executed in conjunction with the police and National Security resources, the Treasury can authorise the unfreezing of funds or economic assets relating to a false positive.
- g. De-listing and unfreezing decisions taken in accordance with European regulations are published in the Official Journal of the EU and the updated list of designated persons and entities is published on a dedicated site. Decisions for removal from the Belgian list and to unfreeze are published in the Belgian Official Journal (but the matter is a hypothetical one given that there are no names on the Belgian list and existing instructions do not mention them).

a4.21. **Criterion 6.7** – At both the European and national levels, there are procedures in place to authorise access to frozen funds or other assets which have been determined to be necessary for basic expenses, for the payment of certain types of expenses, or for extraordinary expenses.¹⁵

Weighting and conclusion

a4.22. The ability to ensure asset freezing ‘without delay’ is the fundamental difference that distinguishes targeted financial sanctions from seizure measures arising from an ordinary criminal proceeding. Consequently, the shortcomings described for criteria 6.2(e), 6.4 and 6.5a are especially important.

Belgium is partially compliant with R 6.

¹⁵ Regulations 881/2001, Art. 2a, 753/2011, 2580/2001, Art. 5-6), and RD of 28 December 2006, Art. 6.

Recommendation 7 – Targeted financial sanctions related to proliferation

a4.23. The obligations pertaining to R 7 were introduced when the FATF standards were revised in 2012 and therefore were not included in the 2005 evaluation of Belgium. Belgium primarily relies on European legislation for the implementation of R 7. UNSCR 1718 concerning the Democratic People’s Republic of Korea is transposed into European law by Regulation 329/2007, and Council decisions 2013/183/CFSP and 2010/413. UNSCR 1737 concerning the Islamic Republic of Iran is transposed into European law by Regulation 267/2012.

a4.24. **Criterion 7.1** – R 7 requires the implementation of targeted financial sanctions “without delay”, meaning in this context, ‘ideally, within a few hours’. Although European regulations are implemented immediately in all EU Member States upon the publication of decisions in the Official Journal of the EU, there are delays in the transposition into European law of UN decisions (a detailed analysis of these delays appears in R 6). However, the problem is alleviated in the case of targeted sanctions relating to proliferation, because UN designation are rare and the EU applies sanctions to a large number of entities that are not concerned by a UN designation. Moreover, the European procedure for prior authorisation of transactions with Iranian entities also allows authorities to refuse authorisation for any transactions with entities designated by the UN but not yet designated at the European level.

a4.25. **Criterion 7.2** – The Treasury Administration within FPS Finance is the competent national authority in charge of implementing and enforcing targeted financial sanctions.

- a. European regulations are applicable to all natural persons who are EU citizens and to all legal persons established or formed under the law of a Member State or associated with a commercial transaction carried out in the EU (Regulation 267/2012, Art. 49 and Regulation 329/2007, Art. 16). The freezing obligation is activated upon publication of the regulations in the Official Journal of the EU. The delays in transposition described above raise the question of compliance with the obligation to execute freezing measures ‘without prior notice’, which deprives the European regulations of any surprise effect.
- b. The freezing obligation applies to all types of funds.
- c. The regulations prohibit making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorised or notified in compliance with the relevant UN resolutions (Regulation 329/2007 Art. 6.4 and Regulation 267/2012 Art. 23.3).
- d. The lists of designated persons and entities are communicated to financial institutions and DNFBPs through the publication of a consolidated list on the EU site at: http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf. The EU also published EU Best Practices for the effective implementation of restrictive measures.¹⁶ In 2009, the Treasury Administration published a notice in the Belgian Official Journal to reiterate obligations relating to the enforcement of restrictive measures (see R 6). The CTIF mentions the obligations relating to R 7 on its web site and in its Guidelines and regularly publishes on its web site warnings about certain sensitive regions or persons affected by embargos. FPS Foreign Affairs also provides a dedicated page on sanctions, including a Manual on Trade with Iran for businesses.¹⁷ The authorities indicate that the Belgian Federation for the Financial Sector sends circulars to its members whenever a new embargo is issued and reminds them of their notification obligations (<https://www.febelfin.be/fr/embargos>). This site provides a chronological inventory of European freezing decisions by country or topic. Information about the updated

16 <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011679%202007%20INIT>.

17 http://diplomatie.belgium.be/fr/politique/themes_politiques/paix_et_securite/sanctions/.

lists can also be communicated to professionals via professional associations (as may be the case for the accounting/tax and legal professions), but these practices do not seem to be harmonised or systematic.

- e. The natural and legal persons targeted by the European regulations must immediately provide all information that will facilitate observance of the EU regulations, including information about the frozen accounts and amounts (Regulation 329/2007, Art. 10 and Regulation 267/2012, Art.40). In addition, the European regulations ask financial institutions, in the framework of their dealings with banks and financial institutions domiciled in Iran, as well as with their branches and agencies abroad, that if they suspect or have good reason to suspect that funds are associated with financing the proliferation of sensitive nuclear activities or with the development of vectors for nuclear weapons, they should quickly report their suspicions to the FIU or to another competent authority designated by the Member State in question (Regulation 267/2012, Art. 32 and Regulation 329/2007, Art. 11a).
- f. The rights of bona fide third parties are protected (Regulation 329/2007, Art. 11 and Regulation 267/2012, Art. 42).

a4.26. **Criterion 7.3** – EU Member States are required to take all necessary measures to ensure that the EU regulations on this matter are implemented and to determine a system of effective, proportionate and dissuasive sanctions (Regulation 329/2007, Art. 14 and Regulation 267/2012, Art. 47). The Law of 13 May 2003 relating to the implementation of restrictive measures adopted by the EU Council against some States, persons and entities, stipulates that, without prejudice to the application of more severe sanctions, offences relating to the measures contained in the regulations on proliferation are punishable by imprisonment ranging from eight days to five years and by a fine of EUR 25 to EUR 25 000 (Art.6). Art.7 stipulates: ‘Without prejudice to the powers of judicial police officers and AGDA agents , agents commissioned for this purpose by the competent minister are tasked with investigating and prosecuting, even alone, violations of the measures taken under the present law’. No agents have been commissioned. Therefore the police and AGDA are solely responsible for investigating offences, but it is not established whether they have adopted measures to monitor compliance with the laws implementing the obligations created by R 7.

a4.27. The Belgian authorities indicate that because the AML/CFT Law does not explicitly address combatting PF, the sanctions set forth under Art.40 of the law could not be applied in the case of non-compliance that is specifically and exclusively related to the organisation and internal audit obligations meant to ensure compliance with European regulations on the proliferation of weapons of mass destruction. Nevertheless, in such a situation, because the same procedures and internal audits would have to simultaneously ensure compliance with the European regulations on the freezing of assets of terrorists and terrorist organisations, the financial institution in question would be automatically and simultaneously in violation of these obligations and could be sanctioned for that reason. Based on these legal considerations, the [CBFA circular](#) specifies that both the customer acceptance policy (point 5.1) and the due diligence requirements relating to business relationships (points 6.1.1 and 6.1.2) must enable financial institutions to ensure that they will satisfy their obligations with regard to financial embargos. The effectiveness of this mechanism still needs to be assessed (see MER) and the shortcomings in the monitoring and sanctions scheme that are identified in R 26, R 28 and R 35 are relevant in the context of R 7. Still, the application of sanctions for a single instance of the non-application of freezing decisions without systemic failure has not been established.

a4.28. **Criterion 7.4** – The European regulations establish measures and procedures for submitting de-listing requests in cases where the designated persons or entities do not meet or no longer meet the designation criteria.

- a. The EU Council communicates its designation decisions, including the grounds for inclusion, to the designated persons or entities who have the right to comment on them. If this is the case or if new substantial proof is presented, the Council must reconsider its decision. Individual de-listing requests must be processed upon receipt, in compliance with the applicable legal instrument and EU Best Practices for the effective implementation of restrictive measures. Designated persons or entities are notified of the Council decision

A4

and can use this information to support a de-listing request filed with the UN (notably via the Focal Point established pursuant to UNSCR 1730/2006). When the UN decides to de-list a person, the Commission modifies the lists in the annexes of the European regulations without the person in question having to request it (Regulation 329/2007, Art. 13.1 (d) and (e) and Regulation 267/2012, Art. 46). The listed persons or entities can file an appeal with the European Court of Justice to challenge the decision to add them to the list.

- b. There is a procedure by which financial institutions notify the Treasury as soon as they observe the name of one of their customers on the list. The procedure involving the Treasury is a procedure for identity verification and information exchange with the police and National Security. It is not certain that these procedures are publicly known.

a4.29. **Criterion 7.5:**

- a. The European regulations permit the payment to the frozen accounts 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 (Regulation 329/2007, Art. 9 and Regulation 267/2012, Art. 29).
- b. Furthermore, concerning freezing measures taken pursuant to UNSCR 1737, special provisions authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation (and *de facto* the Resolution), and after prior notice is given to the UN Sanctions Committee (Regulation 267/2012, Art. 24 and 25).

Weighting and conclusion

a4.30. As for R 6, the ability to ensure asset freezing *without delay* is the element that distinguishes targeted financial sanctions from other measures relating to criminal proceedings. Therefore criteria 7.1 and 7.2 are fundamental components of R 7. **Belgium is partially compliant with R 7.**

Recommendation 8 – Non-profit organisations (NPOs)

a4.31. In 2005 Belgium was deemed to be compliant with the standard pertaining to NPOs (formerly SR VIII; Para. 747 and s. MER 2005). In Belgium, the non-profit organisation (NPO) sector as defined in the Recommendations *Glossary* includes: 1) public interest foundations and private foundations (see R 24), and non-profit associations (NPAs) that are groups of natural or legal persons pursuing altruistic goals and include international non-profit associations (INPAs).

a4.32. **Criterion 8.1** – Since 2004 Belgium has not conducted or updated an examination of its NPO sector with regard to AML/CFT and the potential abusive use of the sector for criminal purposes. Nevertheless, the assessment of the TF threat conducted in February 2014 provides some information about the vulnerability of certain types of NPOs in relation to TF. The CTIF also has information on this matter.

a4.33. **Criterion 8.2** – An initiative to educate the NPO sector about the problem of TF was carried out in the national press in September 2012 by the Minister of Justice. A newsletter meant to inform NPOs about this issue was disseminated. In the fight against TF, in 2005 the Federal Prosecutor's office opened a proactive investigation into a list of NPOs about which there were TF suspicions. No similar action has been carried out since that date. It would be advisable to conduct such initiatives on a more continuous and structured basis with entities from the NPO sector, notably those identified to be at higher risk.

a4.34. **Criterion 8.3** – The Law of 2 May 2002 which organises the NPO sector sets out elements to promote transparency (see C.8.4), notably the keeping of a file on each foundation and NPA/INPA that is maintained by the Commercial Court Registry. The larger NPAs, INPAs and foundations are subject to the

A4

same accounting rules as commercial enterprises¹⁸ and the ‘smaller’ ones are subject to simplified accounting rules. All are subject to audits by the tax authorities. Furthermore, NPOs, regardless of their size, must request authorisation to receive donations and bequests in excess of EUR 100 000. The existing measures help to promote transparency regarding the functioning and management of NPOs and to encourage public confidence, but in a limited manner with regard to small NPOs.

a4.35. **Criterion 8.4** – The obligations described below apply to ‘large’ NPOs. NPOs are required to *a)* maintain information on the purpose and objectives of their stated activities and the identity of person(s) who direct their activities (senior officers and board members). This information is published in the Belgian Official Journal and submitted to the BCE and are therefore available to the public. Information about the identity of persons who control or own NPOs must be collected by financial and non-financial professions pursuant to their AML obligations (see *e*). *b)* The annual financial statements of ‘large’ associations and foundation are filed with the BNB. *c)* The NPOs are required to entrust one or several registered auditors with auditing their financial situation, annual financial statements and the conformity of their operations with laws and statutes. The registered auditor can refuse to certify the accounts or may do so with reservations when irregularities are observed. In the context of detecting ‘false NPOs’ that conduct *de facto* for-profit activities, an audit of the statutes of the activities actually carried out and of the accounts kept by the legal person can be conducted by the tax authorities. *d)* The creation of an NPO triggers the opening of a file with the Commercial Court (see C.8.3). The articles of association of these NPOs and changes to them are published in the Belgian Official Journal. *e)* The requirements of the AML Law regarding the identification of the effective beneficiaries of legal persons apply to NPOs (see C.10.10). *f)* NPOs, INPAS and foundation, regardless of their size, are required to retain accounting documents pertaining to their activities for a period of 7 years. These documents are available to the competent authorities. Nevertheless, the information gathered is not sufficient to guarantee that all the funds are duly accounted for and used in compliance with the stated purpose and objectives of the NPOs.

a4.36. **Criterion 8.5** – Under the Law of 2 May 2002, NPOs can be sanctioned with invalidity, non-allocation of donations (for the case of associations) or dissolution (notably in the event of non-compliance with the requirements to publish information in the Belgian Official Journal, including financial information). During its audits of NPOs, the tax auditor may report facts to the public prosecutor’s office and impose a range of criminal and administrative sanctions. It should be noted that the application of such sanctions does not exclude, where applicable, parallel civil or administrative procedures – which may include dissolution – or criminal procedures against NPOs or persons acting on their behalf. Because of their legal personality, NPOs are in particular criminally liable for offences they commit in pursuit of their corporate purpose or in promoting their interests or on their own behalf. The audits conducted by the Registry of the Commercial Court when an NPO is formed or over the course of its existence, as well as audits of its accounts by the BNB (see C.8.4.b) amount to purely formal audits of the information communicated and do not allow for the verification of whether the funds are used in accordance with the stated purpose and objectives of activities. National Security conducts investigations into INPAS and public interest foundations, but at the stage when they are created and register their legal personalities. The proportionate nature of sanctions applicable to NPOs is not entirely established. The quality and regularity of efforts to ensure NPOs fulfil their obligations are also not demonstrated.

a4.37. **Criterion 8.6** – (a) Mechanisms exist to promote co-operation, co-ordination and information sharing at the national level between the authorities that have relevant information on NPOs. This is notably the case between National Security, the Federal Police and the CTIF (see R 29). Nevertheless, these mechanisms do not seem entirely satisfactory to the extent that they are organised, for the most part, on an informal basis. *b)* The documents pertaining to NPOs held at the Registry of the Commercial Court and published in the Belgian Official Journal can be accessed quickly by the competent authorities in the framework of prevent actions or investigations. *c)* The mechanism for filing suspicious transaction reports (see R 20) can also help notify the authorities and open investigations, where applicable, into NPOs suspected of ML/TF. These same authorities

18 These categories are defined according to criteria pertaining to the number of employees, total revenue and balance sheet (BNB, nd).

can exercise their investigation powers to access information about NPOs that is held by financial and non-financial institutions (see R 31).

a4.38. **Criterion 8.7** – Belgium uses the traditional procedures and mechanisms for international co-operation to respond to third country requests regarding Belgian NPOs or assets in Belgium suspected of financing terrorism. Belgium has not established any specific point(s) of contact – the CTIF and the public prosecutor’s office perform this role in practice – to respond to requests for international information, its 2012 awareness campaign having been limited to communicating a list of the Belgian authorities that can be contacted for any question relating to NPOs.

Weighting and conclusion

a4.39. The initiatives to raise awareness among NPOs about TF are insufficient, as are initiatives pertaining to the periodic reassessment of their TF vulnerability, which are key elements in the prevention of misuse in this exposed sector, as acknowledged by the overall risk assessment conducted at the national level. Furthermore, there are also shortcomings in the monitoring of NPO transparency, notably those at most risk. **Belgium is partially compliant with R 8.**

Bibliography

(BNB, nd). *Critères de taille pour les associations et fondations*, BNB, Brussels,
www.BNB.be/pub/03_00_00_00_00/03_04_00_00_00/03_04_01_00_00/03_04_01_05_00.htm?l=fr.



5. PREVENTIVE MEASURES

Recommendation 9 – Financial institution secrecy laws

a5.1. Belgium was rated compliant in its third assessment (FATF, 2005, para. 399ff).

a5.2. **Criterion 9.1** – There is no ‘banking secrecy’ *per se* but a contractual duty of confidence 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 gives way when personal data must be processed in order for person responsible for handling that information to comply by or pursuant to the provisions of laws or regulations, which is the case when information is required in AML/CFT matters (e.g. Art.3 §5, 4° of the law of 8 December 1992).

Weighting and conclusion

a5.3. **Belgium is compliant with R 9.**

Customer Due Diligence and Record-Keeping

Recommendation 10 – Customer Due Diligence

a5.4. Belgium was rated largely compliant in the third evaluation (para. 383ff. MER 2005). Some desirable improvements were noted concerning, in particular, the application of due diligence measures by consumer credit and leasing companies, and the need for a binding instrument specifying that the exemption from customer identification did not apply in the case of transactions presenting a connection with non-cooperative countries.¹ It should be noted that no regulatory provision has yet been adopted for consumer credit and leasing companies (see C.26.1). This shortcoming should be taken into account in the assessment of preventive measures, given the risks involved in these activities.

a5.5. **Criterion 10.1** – Belgian provisions prohibit the opening of anonymous accounts or accounts under obviously fictitious names (Art. 5 of the Regulation of 23 February 2010 [‘the Regulation’] applying the AML/CFT Law to financial institutions, and Art. 7 of the MD of 10 January 2014 applying the AML/CFT Law to Bpost as regards postal financial services).

a5.6. **Criterion 10.2** – The due diligence obligation incumbent for financial institutions is included in legislation (Art. 7 §1 sub-para. 1 1° to 4° of the AML/CFT Law).² It applies in the situations provided for by R 10, with a threshold of EUR 10 000 for occasional transactions.

a5.7. **Criterion 10.3** – The documentary evidence required for identification and identity verification are specified by regulations for both natural and legal person customers. In general, official documents are required. For natural persons, these are valid identity documents, issued by a public authority (Art. 7 §1 of the Regulation and 9 of the MO). Certain documents require certification in the case of non-face-to-face transactions. These transactions also require additional verification measures (Art. 16 §3 of the Law, Art. 7 §2 of the Regulation and 8 §2 of the MO). Regarding legal person customers, the regulations refer to

1 The other shortcoming noted relative to beneficial owners is not mentioned here as it relates to the implementation of existing measures.

2 Requirement under R 10, footnote 30 (FATF, 2012).

PREVENTIVE MEASURES

documents which, under Belgian law, establish the existence and main characteristics of these legal persons, or to equivalent documents required by the foreign law to which the customer is subject (Art. 8 of the Regulation and 10 of the MO). Reliability of sources used is improved where a notary is involved in preparing the documents relative to legal person identification and has checked the information provided.

a5.8. **Criterion 10.4** – The AML/CFT law requires identification and verification of the customer's representatives, i.e. persons acting in any capacity whatsoever for him and on his behalf, using documentary evidence (Art. 7 §2). Financial institutions must also examine the powers of representation of the person acting on the customer's behalf and verify such powers with supporting documents of which they take copies (Art. 13 para. 2 of the Regulation and 11 of the MO).

a5.9. **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. 8 §1 sub-para. 1). The definition of beneficial owner refers to the identification of a natural person (Art. 8 §2). In order to determine the beneficial owner's identity, in addition to 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 public register of companies (BCE) (C.24.6.). Such sources are not available for customers that are legal arrangements. Financial institutions must define adequate risk-based measures in their internal procedures to verify the identity of beneficial owners (Art. 14 para. 1 of the Regulation and 6 of the MO). If the beneficial owners' identity cannot be verified by means of a conclusive document, the financial institutions specify in internal procedures the other documents or information sources that they rely on and use for the verification, such as indirect access to the National Register³ for example, which allows the beneficial owner's identity to be verified, without concerning the prior requirement of determining his existence and identity. Where the measures stipulated in the internal procedures are implemented but did not enable the identity of a customer's beneficial owners to be verified, the institution should keep written records of the measures effectively taken, to be able to subsequently prove that they were adequate and risk-based.

a5.10. **Criterion 10.6** – The AML/CFT Law provides that customer identification also includes the purpose and intended nature of the business relationship (Art. 7 §1-5). 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 all useful and relevant information revealing the ultimate purpose of this relationship from the customer's standpoint.

a5.11. **Criterion 10.7** – *a)* The AML/CFT Law requires financial institutions to exercise ongoing due diligence with regard to the business relationship and scrutinise transactions undertaken and, where necessary, the source of funds (Art. 14 §1 sub-para. 1). In addition, financial institutions must pay particular attention to any transaction they regard as particularly likely to be connected with ML/TF ('unusual transactions'⁴) (Art. 14 §1 sub-para. 2). *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. 30 of the Regulation). This obligation also applies in respect of information concerning customers' beneficial owners (Art. 8 §2 of the law). In the case of companies, legal persons and arrangements, information about beneficial owners is updated at the financial institution's request (Art. 8 §3).

a5.12. **Criterion 10.8** – There is no explicit requirement for financial institutions to understand the nature of the customer's business or be aware of its control and ownership structure in the case of legal

A5

3 The National Register is a data processing system which records, stores and communicates information about the identification of natural persons. Persons entered in the population registers or registers of foreign persons kept in the communes and persons entered in the registers kept in Belgian diplomatic missions and consular posts abroad are included in the register. Each person is given an ID number when first registered. The data entered and kept in the Register for each person includes: their first and last name; plate and date of birth; main residence; occupation.

4 Refer to the definition in Art. 1 of the Regulation and the MD.

persons or arrangements. However, this information is among some of the elements necessary to implement the customer acceptance policy and ongoing due diligence (Art. 12 of the Regulation⁵) and to identify the beneficial owners (Art. 8 of the Law).

a5.13. **Criterion 10.9** – The identification and verification of legal persons and arrangements concerns the required information (Art. 7 §1 sub-para. 4 of the AML/CFT law), including the identification and verification of the identity of the person (s) acting in any capacity whatsoever for and on behalf of the legal person or arrangement (Art. 7. §2 – see C.10.4).

a5.14. **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 (Art. 8 §1 sub-para. 3 1°). It does not specify whether the financial institution must identify the company's senior managing official where no natural person can be identified by applying *a)* and *b)* (insofar as the function of *member of the board of directors* is different from *senior managing official*). Customer companies are required to inform the financial institution of the identity of their beneficial owners (Art. 8 §3 sub-para. 1 and c. 10.5).

a5.15. **Criterion 10.11** – In the definition of beneficial owner of legal persons other than companies, the AML/CFT Law includes persons who own at least 25% of the legal person's or arrangement's assets, persons in whose main interest the legal person was formed or acts, and persons who exercise control over at least 25% of the assets (Art. 8 §1 sub-para. 3 2°). Under Art. 8 §3 of the law, the relevant legal persons or 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. 8 §3 sub-para. 2), see C.10.10.

a5.16. **Criterion 10.12** – Neither the law nor the regulation contain any specific provision concerning the identification of a 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 (Art. 7 and 8 of the AML/CFT Law). The identification and verification of the beneficiary to whom the benefit will be paid under the life-insurance policy may be done 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 to be one of the beneficial owners (Art. 20 para. 1 of the Regulation).

a5.17. **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 they determine whether enhanced due diligence should be applied. However, financial institutions have a general duty to implement enhanced due diligence in all situations that may present a high risk (Art. 12 §1 of the AML/CFT law). Where the characteristics of the beneficiary of the life-insurance policy (pursuant to the criteria of Art. 26 of the Regulation) suggest that the business relationship involves higher risks, enhanced due diligence, including identification of the beneficial owner, is required, see C.10.12.

a5.18. **Criterion 10.14** – Art.3 of the Regulation 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. 3 para. 2) provides that the circumstances which warrant postponing the verification must be such that the activities between the financial institution and the customer must not be interrupted. In this case, the identity verification must be done as soon as possible after the first contact with the customer, and enhanced due diligence measures must be applied so that the ML/TF risks are effectively controlled.

a5.19. **Criterion 10.15** – Financial institutions wishing to defer verifying a customer's identity must first define the particular circumstances in their internal procedures and specify the precise conditions in

5 Also refer to point 4.2.6.2. CBFA circular "*information about the profession or the economic activity*".

PREVENTIVE MEASURES

their customer acceptance policy, under the control and responsibility of the AML/CFT officer (Art. 3 of the Regulation). Enhanced due diligence must be applied until the identity of all the persons involved has been verified (see C.10.14).

a5.20. **Criterion 10.16** – The law of 18 January 2010 makes provision for transition measures so that the new provisions are implemented by financial institutions in respect of existing customers (Art. 44). The five-year period for financial institutions to record customers' date and place of birth information (Art. 44 para. 1) raises questions, even where there is no high risk and insofar as the financial institution already knew the information. For the identification of beneficial owners, the times allowed for compliance have been set on a risk-sensitive basis, such that they should be less than two years in the case of high risks (Art. 44 para. 2).

a5.21. **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. 12 §1). For certain particular situations (PEPs, correspondent banking), minimum enhanced measures are stipulated, including obtaining authorisation to establish the business relationship or to perform the transaction from an appropriate management level (Art. 12 §3 and 4). 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. 26 of the Regulation), and which fully take higher-risk situations into account.

a5.22. **Criterion 10.18** – The Belgian authorities state that reduced due diligence measures apply for the customer categories referred to in Art. 11 §1 of the law. This provision should be read in combination with §3 sub-para. 1 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 identity of the customer, albeit simplified. However, these situations are based on a presumption of relatively low risk, without a national or supranational analysis of risks associated with each category being produced, which would establish the lowest ML/TF risk.⁶ In any event, the provisions of Art. 11 §1 cannot be applied where ML/TF suspicions arise (Art. 11 §3 sub-para. 2).

a5.23. **Criterion 10.19** – The law provides that where financial institutions are unable to fulfil their obligation to identify the customer or the beneficial owner, they may not enter into or continue a business relationship, or perform any transaction with the customer (Art. 7 §4). In these cases, financial institutions must determine whether it is necessary to inform the CTIF (Art. 8 §4).

a5.24. **Criterion 10.20** – Belgian AML/CFT legislation does not contain any provision permitting financial institutions not to identify 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 customer due diligence.

Weighting and conclusion

a5.25. **Belgium is largely compliant with R 10.**

Recommendation 11 – Record-keeping

a5.26. Belgian was rated compliant with the FATF requirements in the third evaluation (para. 404ff. MER 2005).

a5.27. **Criterion 11.1** – Record-keeping rules are established by the AML/CFT Law (Art. 15) and require that all financial institutions keep all documents necessary to reconstruct transactions for five years after

⁶ The Belgian authorities add that the Belgian law will be adapted, in accordance with the 4th Directive in development, in order to make it clearer that in the case of lower risks, simplified identification and verification obligations apply.

the transactions are carried out. This includes national and international transactions carried out by the customer.

a5.28. **Criterion 11.2** – The legislative framework requires keeping the supporting documentation that served to verify the identity of the customer, its representative and the beneficial owners for five years after the end of the relationship with the customer (Art. 13). One alternative consists in retaining records of the references of documentary evidence, provided that the documents can be produced immediately, and can neither be altered nor modified by the financial institution (Art. 38 §2; Art. 25 of the Regulation and 13 of the MO). Furthermore, there is a general requirement to keep all transaction records, forms and documents, including business correspondence, for five years after the transaction (Art. 15). Accounting law also requires companies, including financial institutions to keep supporting evidence of any accounting entry for seven years.

a5.29. **Criterion 11.3** – The data kept must enable customer transactions to be accurately reconstructed. All documents kept by a financial institution in connection with individual transactions may also serve as evidence in the event of prosecution (Art. 15).

a5.30. **Criterion 11.4** – Financial institutions must take the necessary measures to respond swiftly, and in a complete and adequate manner, to requests for information made by competent authorities (Art. 15).

Weighting and conclusion

a5.31. **Belgium is compliant with R 11.**

Additional measures in the case of specific customers and activities

Recommendation 12 – Politically exposed persons (PEP)

a5.32. Belgium was rated largely compliant in the third assessment (para. 387 MER 2005). The report emphasised that the more stringent acceptance measures applicable to PEPs should also apply to beneficial owners having PEP status. In addition, requirements to identify PEPs did not apply to consumer credit and leasing companies, even though they were subject to the AML/CFT Law. The new FATF requirements extend the applicable measures to domestic PEPs and to international organisation PEPs.

a5.33. **Criterion 12.1** – The definition of PEPs in the AML/CFT Law has limitations, insofar as it lays down a condition of territoriality: persons are only be considered PEPs when they are or have been entrusted with prominent public functions and they reside abroad (Art. 12 §3 sub-para. 1). Application of the FATF measures relating to foreign PEPs is therefore restricted. The definition also includes a one-year limitation after which a PEP who has ceased his functions should no longer be considered a PEP (Art. 12 §3 sub-para. 3). Thereafter, the general principle of enhanced measures applies in the event of higher risks (Art. 12 §1 sub-para. 1). The Belgian system requires a system to detect PEPs, reasonable measures to determine the origin of the customer's or its beneficial owner's funds and wealth, and ongoing monitoring of the business relationship (Art. 12 §3 sub-para. 6). The decision granting authorisation to enter into the business relationship must be made 'at an appropriate level of management'.

a5.34. **Criterion 12.2** – The definition of PEP and particularly the criterion tied to residence abroad does not directly include, *per se*, domestic PEPs or persons who are or have been entrusted with prominent public functions within and for an international organisation covered by the PEP measures.⁷ The Belgian authorities pointed out that as part of the general AML/CFT framework, enhanced due diligence measures

⁷ The Belgian authorities state their intention to adapt the PEP system via the transposition of the 4th AML/CFT Directive currently being prepared.

PREVENTIVE MEASURES

can be applied in higher-risk situations (Art. 12 §1); this implies the determination of a risk profile and thus could be applied in situations involving domestic PEPs or persons who are or who have been entrusted with a prominent function within and for an international organisation. The customer risk profile is determined according to individual criteria at each financial institution, which may include – although there is no relevant obligation in the law – the customer’s profession or sector of activity, as well as his/her source(s) of income. The identification of domestic PEPs or PEPs from international organisations is therefore only indirect under these circumstances.

a5.35. **Criterion 12.3** – The Belgian law restrictively lists persons who must be considered immediate family members of PEPs and persons closely associated with them (Art. 12 §3 sub-paragraph 4 and 5). This approach is restrictive compared to the FATF’s open approach which covers all individual situations involving specific risks owing to their ties with a PEP. In addition, the same reservations as those expressed in C.12.1 and C.12.2 should be considered with respect to the scope of application of the legislative provisions and the due diligence measures to be adopted.

a5.36. **Criterion 12.4** – The Belgian system does not contain any specific provisions requiring financial institutions to verify whether the beneficiary of a life-insurance contract, or its beneficial owner, is a PEP. The system does, however, require enhanced due diligence in all situations which, by their nature, are a high ML/TF risk (Art. 12 §1), which may be the case if the financial institution determines that the beneficiary of a life-insurance policy, or its beneficial owner, is a PEP.⁸

Weighting and conclusion

a5.37. Several shortcomings are to be observed: The PEPs definition in the law does not include domestic PEPs or persons who are or have been entrusted with prominent functions in an international organisation. Furthermore, the law includes a limited list of persons who should be considered as a direct member of the family of a PEP and persons closely associated. The definition of a PEP of one year after which a PEP having stopped his/her functions should no longer be considered a PEP. Finally, there are no provisions in the Belgium system that specifically require financial institutions to verify that the beneficiary of a life-insurance policy or the beneficial owner thereof is a PEP. These shortcomings may be attenuated in practice – however not systematically, as the practice is based on the risk analysis carried out by financial institutions – by the general requirement to determine the customer’s risk profile and to apply enhanced due diligence in situations of higher risk. All of these gaps together are considered to be a moderate shortcoming, given their extent with regard to the FATF requirements and their importance in the area of enhanced due diligence.

Belgium is partially compliant with R 12.

Recommendation 13 – Correspondent banking

a5.38. Belgium was rated compliant in the third evaluation (para. 367ff. MER 2005). The new FATF Recommendation adds requirements relative to prohibiting business relationships with shell banks.

a5.39. **Criterion 13.1** – The law requires enhanced due diligence measures when entering into correspondent banking relationships (Art. 12 §4)^{9,10} with institutions from a third country in the manner specified by R 13. These measures do not apply to correspondent banking with financial institutions from another EEA Member State or a third country that imposes obligations and require monitoring equivalent to those stipulated by

A5

8 The Belgian authorities state their intention to introduce additional measures, when the adaptation of the system applicable to PEPs will be contemplated more generally as part of the transposition of the 4th AML/CFT Directive being prepared.

9 Bpost does not open accounts for foreign financial institutions to which it offers correspondent banking services.

10 The Belgian authorities state their intention to examine the possibility of adapting the applicable system overall, based on the new European framework being defined.

the third AML/CFT Directive. In addition, the measures provide for an exemption from identification and verification of the client and of the beneficial owner (Art. 11 §1 1°). The RD that sets out the list of third-country equivalents (RD of 19 July 2013) specifies, in a recital which cannot be considered to be legally binding, that this exemption does not apply in situations considered to be high risk.

a5.40. **Criterion 13.2** – Where a correspondent banking relationship involves the maintenance of payable-through accounts, the AML/CFT Law requires Belgian financial institutions to be satisfied, firstly, that the foreign institution has verified the identity of 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.12 §4 sub-para. 1 5°).

a5.41. **Criterion 13.3** – The law provides that financial institutions may not enter into or continue a correspondent banking relationship with a shell bank,¹¹ 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. 12 §4-2).

Weighting and conclusion

a5.42. The specific diligence measures required in the area of correspondent banking apply in the case of business relationships with financial institutions located in a third country considered to be high risk. Nonetheless and pursuant to Art.12 § 4 of the law which applies ‘without prejudice... exemptions referred to in Art.11 § 1 1°’, they do not apply in relations with EEA institutions or in third-country equivalents. Given the open and cross-border nature of the Belgian banking sector and the fact that the Recommendations consider cross-border correspondent banking as a high risk activity, the shortcomings are moderate. **Belgium is partially compliant with R 13.**

Recommendation 14 – Money or value transfer services

a5.43. Belgium was rated compliant in the third evaluation (para. 578ff. MER 2005). The law of 21 December 2009 transposed Directives 2007/64 on payment services (PSD I) and 2009/110 on electronic money institutions, which directly impacted regulations applicable to money remittance services. R 14 lays down new requirements relating particularly to the identification of non-authorised or non-registered MVTS providers, and to the definition of sanctions for failure to comply with these requirements.

a5.44. **Criterion 14.1** – Payment services are listed in Annex I to the law of 21 December 2009 and include money transfers. BNB, the ECB, the Belgian federal, regional, community and local authorities when they are not acting as public authorities, and Bpost, are among the institutions authorised by law to provide payment services (Art. 5), without the need to obtain prior authorisation owing to their status. The other financial institutions offering money transfer services covered by Annex I to the law - credit institutions, electronic money institutions and payment institutions – are subject to a requirement to obtain authorisation from the BNB (R 26). Institutions that 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 (Art. 48 and 105 of the law of 21 December 2009). Annex I of the law also covers credit and electronic money institutions governed by the laws of another EEA Member State and which offer payment services in Belgium through branches, or under freedom to provide services (Art. 5 1° and 2°). Under the principle of mutual recognition, they are authorised to provide these services, where the authorisation granted in their original Member State so permits. The BNB is notified by the authority in the

11 The law does not explicitly define the notion of ‘shell bank’ but the presentation of the reasons for the draft law specifies that: *Pursuant to Article 3.10 of the Directive [2005/60/CE], ‘shell bank’ shall be understood as meaning: a credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is unaffiliated with a regulated financial group* - Chamber of Representatives (2009), p. 46.

PREVENTIVE MEASURES

original Member State that such companies intend to carry on activities in Belgium (Art. 312 and 313 of the law of 25 April 2014, and 39 and 91 of the law of 21 December 2009).¹² Branches of institutions governed by the laws of a non-EEA country are also permitted to provide payment services in Belgium (Art. 5 1° and 2° of the law of 21 December 2009), by virtue of the banking licence they are granted by the BNB in Belgium (Art. 333 of the law of 25 April 2014, and 98ff. of the law of 21 December 2009).

a5.45. **Criterion 14.2** – The FSMA is responsible for contributing to compliance with rules aiming to protect users of financial products or services and borrowers from the unlawful supply of financial products or services and credits (Art. 45 §1 5° of the law of 2 August 2002). If, when analysing files within its remit, the CTIF identifies persons illegally performing MVTs activities, it may inform the FSMA. The FSMA conducts enquiries to identify and sanction non-registered or non-authorised MVTs providers. Provision is made for criminal sanctions (Art. 51 of the law of 21 December 2009) and administrative sanctions (Art. 86a, §1, 3° of the law of 2 August 2002) for natural or legal persons providing MVTs without being registered or authorised. As there is no clear policy regarding applicable sanctions, the proportional nature thereof cannot be determined.

a5.46. **Criterion 14.3** – Belgian credit institutions, electronic money institutions providing payment services, and payment institutions are under the supervisory authority of the BNB, including in AML/CFT matters, pursuant to the AML/CFT Law (see R 26). Payment institutions and electronic money institutions from another EEA Member State offering payment services in Belgium via agents based in Belgium are subject to the AML/CFT Law (Art. 2, §1 4°ter c and 4°quater e). They must appoint a person responsible for compliance with the Belgian AML/CFT Law, and that person must be based in Belgium (Art. 18 para. 3). The BNB then exercises its supervision through this person, the ‘central contact point’. Bpost acts as agent for a European payment institution for its money transfer operations. This payment institution is therefore subject to the AML/CFT requirements as regards the MVTs activities it performs in Belgium through Bpost. Bpost acts as central contact point for these specific transfer activities, for which it is placed under the supervision of FPS Finance (R 26).¹³ European payment institutions offering services in Belgium under freedom to provide services are subject to supervision by the authority in their original country.

a5.47. **Criterion 14.4** – The law requires payment and electronic money institutions to register their agents (which provide payment services) with the BNB (Art. 20 §1 of the law of 21 December 2009).¹⁴

a5.48. **Criterion 14.5** – The general requirements for organisation and internal control to which financial institutions are subject, as well as the requirements of the AML/CFT Law, cover all the activities that these institutions carry out, regardless of whether they use their own personnel or agents to do so. Agents are contractually required to comply with the rules applicable to their principal (the payment institution), including the AML/CFT policy of that payment institution. The AML/CFT Law (Art. 10 §1) and its implementing regulation (Art. 21) more specifically require the financial institution to monitor compliance with the identification and verification procedures prescribed, where they use the services of an agent.

Weighting and conclusion

a5.49. **Belgium is largely compliant with R 14.**

A5

12 BNB (nd a, b)

13 The same European payment institution has a second network of agents in Belgium for which it has appointed a separate central contact point and comes under BNB supervision.

14 BNB (nd c, d).

Recommendation 15 – New technologies

a5.50. Belgium was rated compliant in the third evaluation (para. 388 MER 2005). However, the new R 15 focuses on preventing risks involved in the use of new technologies in general and no longer specifically targets contracts concluded on a non-face-to-face basis.

a5.51. **Criterion 15.1** – Belgium has not developed any specific analysis of the ML risks to which the financial system is exposed as a result of the use of new technologies, except for the national risk assessments (see R 1). Financial institutions are not explicitly required to identify and assess risks involved in the development of new products and new business practices, including new delivery mechanisms, which use new technologies. However, the risks inherent in using these innovations are taken into account, particularly through the general requirement to take measures based on the eventual high nature of risks. However, consideration of these innovation-related risks cannot be considered fully satisfactory, as it is not an explicit and specific requirement for financial institutions as the legislation currently stands.¹⁵

a5.52. **Criterion 15.2** – a) Financial institutions are not explicitly required to assess risks prior to the launch or use of new products, practices and technologies. b) The general AML/CFT framework allows ML/TF risks involved in using new technologies to be taken into account, by application of the enhanced due diligence rules applicable when concluding contracts remotely, by the definition of ‘specific risk criteria’ underpinning the risk-based approach, and in the initial definition of the customer’s risk profile. This framework allows appropriate measures to be taken to mitigate and manage these risks.¹⁶

Weighting and conclusion

a5.53. **Belgium is largely compliant with R 15.**

Recommendation 16 – Wire transfers

a5.54. Belgium was rated largely compliant in the third evaluation (para. 578ff. MER 2005). The Belgian legislative framework changed substantially in 2006 with the application of the provisions of Regulation 1781/2006 on information relating to the originator which accompanies transfers of funds. The FATF Recommendation (R 16) has also undergone significant changes, and a new European Regulation is currently being prepared to take the new requirements into account, particularly the duty to include and send information about the beneficiary and the broader requirements for intermediate financial institutions. These limitations will be taken into account in all relevant criteria. It shall be noted that the MD for Bpost requires beneficiary identification for postal transfers (Art. 5), but this requirement will not affect ratings given the small volume of these transactions and the fact they are part of Bpost’s public services.

a5.55. R 16 does not apply to transfers carried out using a debit or credit card or a prepaid card for the purchase of goods or services, so long as the credit, debit or prepaid card number accompanies all transfers resulting from the transaction. Regulation 1781/2006 does not contain any explicit provision, but the approach is similar overall.

a5.56. **Criterion 16.1** – Pursuant to the Regulation, all transfers where the payment service provider of the beneficiary is located outside the EEA must be sent with complete information about the originator in the manner required by R 16 (Art. 4 and 7 para. 1). The payment service provider must verify the information

15 The Belgian authorities intend to clarify the current provisions when transposing into domestic law the 4th AML/CFT Directive currently in development.

16 The current legal and regulatory framework should be clarified to take the new FATF requirements into account, which the Belgian authorities intend to do as part of the transposition of the 4th AML/CFT Directive currently being developed.

PREVENTIVE MEASURES

about the originator on the basis of documents, data or information obtained from a reliable and independent source (Art. 5 para. 2). The Regulation does not require the transfer of information about the beneficiary.¹⁷

a5.57. **Criterion 16.2** – For batch transfers carried out by a single originator where the payment service providers of the beneficiary are situated outside the EEA, the Regulation requires the batch file to contain complete information on the originator. Transfers must also include the beneficiary's account number or a unique identifier (Art. 7 para. 2). Neither the Regulation nor the Belgian law currently contains any specific provisions regarding the duty to enclose information about the beneficiary's identity with cross-border batch transfers.

a5.58. **Criterion 16.3** – All the provisions of the Regulation are mandatory and directly applicable in Belgium. Art. 5.4. sets a threshold for transfers that do not originate from an account, and only requires a verification of the originator's identity above EUR 1 000. Below that threshold, originator information, as described in C.16.1. must nonetheless be provided. The same reservations as those made in C.6.1 apply in respect of the requirement for transfers to include information about the originator.

a5.59. **Criterion 16.4** – The AML/CFT Law explicitly requires financial institutions to identify their customers and to verify their identity where there is any suspicion of ML or TF (Art 7 §1 sub-para. 1 3°). Art. 5.4. of the Regulation also states that the exemption from verifying the originator's identity does not apply if there is any suspicion of ML/TF.

a5.60. **Criterion 16.5** – For domestic transfers (within the EEA),¹⁸ the Regulation contains an exemption from the requirement to provide complete originator information (Art. 6.1.). However, the exemption may only apply where complete information about the originator can be made available to the beneficiary's financial institution by other means: at the request of the beneficiary's payment service provider, the originator's payment service provider must be able to furnish complete information about the originator (Art. 6.2.).

a5.61. **Criterion 16.6** – Under the exemption, the transfer may be accompanied solely by the originator's account number or unique identifier allowing the transaction to be traced back to the originator (Art. 6.1.). It must nonetheless be possible for full information about the originator to be sent to the beneficiary's institution within three working days of receiving any request (Art. 6.2.). The Regulation does not, however, currently contain the same requirement concerning information about the beneficiary. The BNB has general power to demand production of any relevant information by the institutions under its supervision and could therefore demand immediate production of information about the originator. Law enforcement authorities also have the power to demand production of information, provided that the conditions required by the criminal procedure, concerning judicial information in particular, are met (Art. 46 *quater* of the CPC).

a5.62. **Criterion 16.7** – The Regulation requires the originator's financial institution to keep the complete originator information which accompanies transfers for five years (Art. 5.5.). In addition, the AML/CFT Law contains a general requirement to retain all information relating to the customer's identification and the documentary evidence used to verify the same, for five years after termination of the contractual relationship or completion of the transaction (Art. 13). The Regulation does not contain any specific provision requiring the retention of beneficiary identification data, even if it has been obtained. The AML/CFT Law does, however,

A5

17 The provisions relating to the beneficiary contained in Reg.260/2012 (SEPA Regulation) are not mandatory and do not address the name of the beneficiary, as regards relations between the payment service provider and its originator-customer (Annex 2 a) iv 'if the information is available, the name of the beneficiary') and between the payment service provider of the originator and the beneficiary (Annex 2 b) vi) 'any identification code of the beneficiary' and vii 'the name of any reference to the beneficiary').

18 Transfers within the EEA covered by the Regulation cover a broader scope than R 16. R 16 requires that all service providers involved be located in the EEA. Art. 6.1. of the Regulation covers transfers for which the payer's and the payee's service providers are located in the EEA. In theory, according to the Regulation, a domestic transfer could therefore be forwarded by an intermediate institution located outside the EEA.

contain a general requirement to keep for five years the documents allowing the transactions performed by the customer to be reconstructed (Art. 15).

a5.63. **Criterion 16.8** – Any failure to comply with the requirements contained in the Regulation is liable for a sanction contained in the AML/CFT Law. The AML/CFT Law also provides that if a covered institution cannot meet its customer due diligence requirements, it may neither enter into nor continue a business relationship, or perform any transaction for the customer (Art.7 §4). However, this due diligence requirement only concerns the originator in the context of money transfers, not the beneficiary.

a5.64. **Criterion 16.9** – The Regulation requires all information received about the originator and accompanying the money transfer, whether domestic or cross-border, to be kept with this transfer by the intermediate service provider (Art. 12). There are no provisions relative to beneficiary information.

a5.65. **Criterion 16.10** – The Regulation provides that where the intermediary payment service provider, located in the EEA, uses a payment system with technical limitations, and where the beneficiary service provider is located outside the EEA, preventing transmission of the originator information with the money transfer, it must keep the information received for five years (Art. 13.5). It may not, however, use such a technical system if it finds that the transfer received has missing or incomplete information (Art. 13. 2 and 3). This requirement does not extend to beneficiary information.

a5.66. **Criterion 16.11** – The Regulation does not specifically require an intermediary financial institution to take reasonable measures to identify cross-border transfers having missing or incomplete information, which in any case only concern originator information in the provisions in force.

a5.67. **Criterion 16.12** – The Regulation does not specifically require an intermediary financial institution to implement a risk-based approach to define the steps to be taken if the required information is not sent with the transfer. However, (intermediary) financial institutions are subject to the general requirement to exercise enhanced due diligence in the case of a higher risk, particularly in the event of atypical transactions (see C.16.15).¹⁹

a5.68. **Criterion 16.13** – The Regulation requires the beneficiary payment service provider to detect whether the fields relating to the originator information have been completed (Art. 8). For cross-border transfers, effective procedures must be in place to detect whether the complete originator information, or, where applicable, the required information in the case of technical limitations, is missing. The Regulation does not contain any requirements regarding the measures to be taken to detect cross-border transfers which do not contain the required beneficiary information. However, as the obligation is incumbent upon the beneficiary's service provider, it can be considered that it will have access to this information and will be able to detect any missing or incomplete beneficiary information.

a5.69. **Criterion 16.14** – The Regulation does not contain any specific provision requiring the beneficiary's financial institution to verify information about the beneficiary's identity, if it has not already been done, and to keep such information. However, for the performance of a wire transfer, the identification of the customer – the beneficiary of the transfer – and the verification of his identity are required, regardless of the amount of the transaction, under the general provisions of the AML/CFT Law (Art. 7 §1). In addition, under the AML/CFT Law, covered financial institutions must keep their customers' identification data, and a copy of the documentary evidence used to verify their identity, for at least five years after termination of the business relationship or performance of the occasional transaction (Art. 15).

a5.70. **Criterion 16.15** – The Regulation does not contain any explicit requirement to adopt a risk-based approach to allow the beneficiary's financial institution to define the steps to be taken when the required information does not accompany the transfer. But in these circumstances, the Regulation requires the

¹⁹ The Belgian authorities specify that the new draft Regulation adapted by the European Commission on 5 February 2013 contains a provision that will in this respect complete the requirements imposed on intermediate beneficiary institutions.

PREVENTIVE MEASURES

beneficiary's financial institution to reject the transfer or to request complete information about the originator (Art. 9.1). The Regulation also requires the beneficiary's payment service provider to consider missing or incomplete originator information as a factor of note in assessing the potentially suspicious nature of a money transfer or any transactions relating thereto, and if applicable, in deciding whether it must be reported to the authorities responsible for AML/CFT (Art. 9.2.). The Belgian regulatory measures adopted to implement the AML/CFT law further specify that a wire transfer received for a customer without being accompanied by information concerning the originator must be considered an 'unusual' transaction, which must prompt the financial institution to consider making an STR to the CTIF. These measures nonetheless target cases in which the missing information concerns the originator (Art. 32 of the Regulation, 18 para. 5 of the MO).

a5.71. **Criterion 16.16** – In Belgium, MVTs are provided by credit, payment or electronic money institutions, authorised to offer this kind of service, and by Bpost (see R 14). The Regulation also applies to money transfers sent or received by a payment service provider established in the EEA. Furthermore, the Regulation and the AML/CFT Law apply to payment service providers established in Belgium, regardless of their form, including when they act through intermediate agents, and whatever the service provider's original country.

a5.72. **Criterion 16.17 – a)** The Regulation does not contain any specific requirement relating to measures to be taken when the payment service provider acts both as the originating entity and beneficiary of the transfer. Where a payment service provider holds information concerning both the originator and the beneficiary, it must take all of this information into account as part of its due diligence in respect of the transaction with a view to determining whether the transaction should be considered 'unusual' and suspicious, and therefore reported to the CTIF. **b)** Given the principle of territoriality of AML/CFT Laws, when a given payment service provider is established in several countries, performs a money transfer between two of its entities, and the transaction proves to be suspicious, it may be required to submit an STR to the FIU in each of these countries pursuant to their respective domestic laws.

a5.73. **Criterion 16.18** – Belgian financial institutions are required to take freezing measures pursuant to UNSCR 1267/1999 and UNSCR 1373/2001 and their subsequent resolutions. This requirement arises both from EU regulations and from a body of domestic provisions. Although such a requirement exists, there are nonetheless serious gaps that could adversely affect the ability of financial institutions to meet their requirements in terms of implementation of targeted financial sanctions (conclusions with regard to R 6).

Weighting and conclusion

a5.74. The absence of any requirements in Regulation 1781/2006 relative to the transmission of beneficiary information is the main shortcoming for C.16.1.-3 and C.16.13 and C.16.15. The lack of requirements for intermediary financial institutions affects C.16.8 and C.16.9. **Belgium is partially compliant with R 16.**

Reliance on third parties, Controls and Financial Groups

Recommendation 17 – Reliance on third parties

a5.75. Belgium was rated compliant in the third evaluation (para. 389ff. MER 2005). The Belgian legislative framework was modified by the law of 18 January 2010 as regards reliance on third-party business introducers, and the revised FATF requirements place the emphasis on the third party's country risk.

a5.76. **Criterion 17.1** – Financial institutions may use the services of third-party introducers in the manner specified in R 17 (Art. 10 §1 of the AML/CFT Law). The requirement that the third party be regulated and subject to AML/CFT supervision is considered to be met by reference to financial institutions in the EEA and equivalent third countries (RD of 19 July 2013). There is a presumption that these financial institutions are subject to regulation and to AML/CFT supervision, but the financial institution should be able to directly verify that the required measures are in place, and be satisfied that the third party effectively performs the

due diligence requirements, particularly those concerning record-keeping to which Art. 24 of the Regulation does not refer.

a5.77. **Criterion 17.2** – The third-party introducer may be based either in Belgium, or in another EEA Member State, or in an equivalent third country (Art. 10 §1 sub-para. 1 of the AML/CFT law). The reliance on financial institutions established in EEA Member States is not based on information relative to the country's ML/TF risks, but reflects the presumption that all EEA Member States implement harmonised AML/CFT provisions. Inclusion on the list of equivalent third countries takes into account the compliance of local legislation with the principal FATF Recommendations, and the degree of risk related to the scale of criminality to which the country is exposed. Account is therefore taken of risk-related factors, without focussing the analysis on ML/TF risks.

a5.78. **Criterion 17.3** – The Belgian framework does not contain any specific measure that changes the way in which a financial institution must meet its requirements when the third party introducer is part of the same financial group.

Weighting and conclusion

a5.79. Under the applicable exemption, the financial institution need not verify that the AML/CFT measures of a third party located in an EEA country or in an equivalent third country are satisfactory, which has an important impact on the rating, particularly as Belgian banking activity is considerably open to relationships with European partners or partners located in equivalent third countries. **Belgium is partially compliant with R 17.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

a5.80. Belgium was rated largely compliant in the third evaluation (para. 471ff. MER 2005). The problem identified was the fact that some elements of the requirements (hiring of staff for internal control measures; compliance with provisions equivalent to Belgian AML/CFT legislation by subsidiaries and branches of Belgian institutions established in non-EU or non-FATF member countries) were specified in a non-compulsory circular. R 18 introduces new requirements regarding the creation of an independent audit function for internal control and AML/CFT programmes for financial groups.

a5.81. **Criterion 18.1** – Financial institutions must implement AML/CFT programmes in the manner required by R 18, with a reservation for the independent internal audit function. Credit institutions, insurance companies, investment companies, electronic money institutions and payment institutions must take the measures necessary to have such a function²⁰ covering AML/CFT measure and procedures at all times. Collective investment schemes and management companies for collective investment schemes must also have an appropriate independent and ongoing audit function which particularly scrutinises risk management.²¹ No reference is made to audit or equivalent functions for the other financial institutions (intermediaries in banking and insurance services, bureaux de change).

a5.82. **Criterion 18.2** – The law requires credit institutions and investment firms to develop a co-ordinated programme and to introduce co-ordinated procedures and structures for the organisation they form with their subsidiaries and branches (Art. 16 §2).²² However, these requirements do not apply when the financial

20 Art. 21 §1 4; 35 §1 and 39 of the law of 25 April 2014, 14bis §3 sub-para. 2 of the law of 9 July 1975 and 62 §3 sub-para. 2 of the law of 6 April 1995, 14 §3 and 69 §3 of the law of 21 December 2009.

21 Art. 41 §4 and 201 §4 of the law of 3 August 2012 and 6 §4 of the RD of 12 November 2012.

22 Belgian legislation appears to consider the notion of group only when it involves institutions abroad (point 10.3.2. para. 1 of the CBFA Circular) but similar principles must also apply to financial groups having some or all of their institutions established in Belgium.

PREVENTIVE MEASURES

group is not headed by a credit institution or an investment firm. The effective content of the requirements to be implemented in this co-ordinated programme is set out in the CBFA Circular which is not mandatory (Art. 19.3 of the law of 22 February 1998).²³ It recommends that the programme include measures concerning control and internal audit, as well as the compliance function, and training of personnel. The provisions relating to the exchange of information within groups do exist, but do not specify any requirements in terms of policies or procedures. On the other hand, requirements concerning the hiring of personnel are not included.

a5.83. **Criterion 18.3** – Measures concerning compliance by subsidiaries and branches with AML/CFT rules compatible with the level required in the original country do exist, but they are only contained in the non-mandatory CBFA circular.

Weighting and conclusion

a5.84. The small size of the institutions for which there is no requirement to create an audit function, reduces the impact of this shortcoming. However, measures organising co-ordination of AML/CFT programmes for groups should be completed insofar as they require the development of a co-ordinated AML/CFT programme only for financial groups which are headed by a credit institution or investment firm and must appear in legislation or regulation. These shortcomings are considered as moderate in the Belgian context which is characterised by a large proportion of financial institutions that are part of financial groups, at the European level for a certain number of them, and for which it is important that AML/CFT programmes be co-ordinated and specified at the group level. **Belgium is partially compliant with R 18.**

Recommendation 19 – Higher-risk countries

a5.85. Belgium was rated compliant in the third evaluation (para. 425 MER 2005). R 19 re-formulates the requirements and introduces new ones concerning the measures to be taken with respect to higher-risk countries.

a5.86. **Criterion 19.1** – Financial institutions are required to submit to a ‘close examination’ (understood to mean enhanced due diligence), with a power of decision at an adequate level of management, which in practice will be a high level (see c.10.17), when entering into business relationships or executing a transaction with customers that are residents in a country considered high risk and/or non-cooperative by FATF or in respect of which FATF recommends countermeasures or enhanced due diligence (Art. 27 of the Regulation and 16 of the MO). Such enhanced due diligence continues throughout the business relationship, under the requirement for ongoing due diligence (Art. 14 of the AML/CFT law, Art. 32 para. 3 of the Regulation). The Belgian authorities state that in the case of a transaction having a connection with a high-risk or non-cooperative country, Art. 11 §1 of the AML/CFT Law, which establishes an exception to the identification requirement for financial institutions established in the EEA or in an equivalent third country, would not apply, since this situation should be considered as involving a greater risk (Art. 27 of the Regulation, 16 of the MO) and thus Art. 12 §1 which requires that enhanced due diligence measures should then apply.

a5.87. **Criterion 19.2 – a)** Art. 27 of the law allows a specific countermeasure to be adopted by royal decree (duty to send information to the FIU), applicable to transactions concerning natural or legal persons domiciled, registered or established in countries for which FATF requires such countermeasures. No such RD has been adopted. The extent of the countermeasures thus imposed must therefore be determined on a risk-sensitive basis when preparing the RD, integrating the type of transaction and setting a minimum amount. Furthermore, Art. 19 restricts the possibility that financial institutions have of setting up in one of the countries referred to, or of entering into business partnerships with entities connected with such

23 Circular of 9 April 2010 which explains the provisions of the AML/CFT law and of the regulation to financial institutions covered – Following the 2010 reorganisation of financial sector supervision in Belgium, the powers of the CBFA (*Commission bancaire, financière et des assurances*) were divided between the BNB and the FSMA. Decisions previously made by the CBFA, particularly the circulars, are however still valid (Art. 329 to 331 of the RD of 3 March 2011) – See R 26.

countries. *b)* Belgium does not, however, have any instruments whereby a countermeasure may be decided independently of an FATF decision.

a5.88. **Criterion 19.3** – The CTIF systematically communicates information on its website for all persons and institutions subject to the AML/CFT Law about the latest decisions made by the FATF in respect of countries with strategic shortcomings in AML/CFT matters. It thus provides information on concerns about weaknesses of the AML/CFT systems of other countries, which are not publicly identified by FATF as a higher-risk country (e.g. Cyprus, Ukraine).

Weighting and conclusion

a5.89. **Belgium is largely compliant with R 19.**

Reporting of Suspicious Transactions

Recommendation 20 – Reporting of suspicious transactions

a5.90. In 2005, Belgium was rated largely compliant with the FATF standard which set out the requirement to report suspicious transactions (former R 13 and SR IV, owing to issues of effectiveness, not technical compliance).

a5.91. **Criterion 20.1** - The AML/CFT law provides that where covered institutions are aware or suspect that a transaction is connected specifically with ML or TF, they must inform the CTIF (Art. 23). Regarding the timing of STRs, in principle they must be made prior to performing the transaction. It may be done afterwards, if the transaction cannot be delayed due to its very nature, or if delaying it is likely to prevent action from being taken against the offenders. In these cases, the CTIF must be notified immediately after executing the transaction and be informed of the reason why the transaction was not reported before being executed.

a5.92. The law also states that where the institutions or persons covered are aware of a fact that could be an indicator of ML/TF, they are to immediately inform the CTIF (this may also be in connection with the intervention of judicial authorities or by the media). The authorities state that the fact that the judicial authorities are aware of the financial transactions in question does not lift the requirement to report them. The slightest suspicion is sufficient for the reporting requirement to apply, for example when the professional cannot rule out a possible connection with ML/TF.

a5.93. Under the AML/CFT Law, ML consists of actions (conversion, concealment, etc.) relating to money from illicit sources. Money from illicit sources is defined with reference to a list of serious offences laid down in Art.5 §3 of the law. Criminal law therefore covers financial benefits derived from any criminal offence (see R 3) whereas the preventive law contains a list of basic crimes which, although very broad and covering all offences punishable by a prison sentence of at least six months, is restrictive. The list of serious offences contained in Art.5 §3 covers all the predicate offences to ML set out in the Glossary of the *FATF Recommendations*. Particularly addressed are offences relating to terrorism and TF as well as serious tax fraud, whether or not organised. In addition, a CTIF guideline clarifies: *Covered institutions, persons and professions are not required to determine the predicate offences to the facts or transactions they detect and for which there is a suspicion of ML or TF. In most cases, reporting parties are not able to know the predicate offence to the transactions they detect. The CTIF is responsible for conducting an in-depth analysis to discover the connection between the reported transaction and one of the crimes covered by the law.* The existence of a list in the AML/CFT Law has no practical consequences.

a5.94. **Criterion 20.2** – The obligation to report suspicious transactions applies in Belgium, regardless of the amount of the transaction. In addition, the law explicitly states that attempts to commit one of the acts defined as constituting ML are acts of ML.



A5

PREVENTIVE MEASURES

Weighting and conclusion

a5.95. **Belgium is compliant with R 20.**

Recommendation 21 – Tipping-off and confidentiality

a5.96. In 2005, Belgium was rated compliant with the FATF standard which set out firstly, the protection of reporting entities when they report their suspicion in good faith to the FIU and, secondly, the duty of confidentiality incumbent upon those same entities (former R 14).

a5.97. **Criterion 21.1** – No civil, criminal or disciplinary action may be brought against and no professional sanction may be imposed on reporting entities or their senior executives, employees or representatives which have reported in good faith to the CTIF. The AML/CFT Law also provides for the protection of reporting parties against any threat, hostile act or intimidation. Lastly, when the CTIF makes a disclosure to the public prosecutor, the federal prosecutor or their foreign counterparts, the STRs (and supplemental STR additional reports) are not legally part of the information sent to the prosecutor so as to maintain the anonymity of the reporting entities.

a5.98. **Criterion 21.2** – Pursuant to Art.30 para. 1 of the AML/CFT Law, reporting entities or their senior executives, employees or representatives may not, under any circumstances, inform the customer in question or other third persons that information has been transmitted to the CTIF under their duty to report suspicious transactions or that a ML or TF investigation is being or may be carried out. Where a professional (notary, auditor, independent certified accountant, independent tax advisor, chartered accountant, licensed tax accountant or lawyer) attempts to dissuade a customer from engaging in illegal activity, this does not amount to tipping-off within the meaning of Art.30 para. 1 (see C.23.4).

Weighting and conclusion

a5.99. **Belgium is compliant with R 21.**

Designated non-financial Businesses and Professions

Recommendation 22 – DNFBPs: Customer due diligence

a5.100. Belgium was rated partially compliant in the third evaluation (para. 589ff. MER 2005). The main shortcomings related to the absence, firstly, of measures implementing the law for a majority of professions, be it the requirement to identify legal persons or PEPs, or specific measures in the event of non-face-to-face contracts, and secondly, of requirements for legal and accounting/tax professions to prepare written reports on unusual transactions.

a5.101. **Criterion 22.1** – Company service providers are not covered by the AML/CFT Law. This sector was identified as at risk, in particular domiciliation companies, and measures are therefore being developed to require licensing and compliance with AML/CFT preventive measures. The due diligence requirements of the AML/CFT Law are applicable to non-financial businesses and professions. The limits identified for financial institutions (see R 10) are thus found in the framework applicable to non-financial businesses and professions. In general, the due diligence measures required by the law are explained in the regulatory provisions applicable to each sector. There are a number of reservations concerning the measures in force. For online casinos, the technical resources currently available do not render verifications of the identity of gamblers totally reliable. A number of ambiguities are noted in the measures applicable to diamond traders,

A5

which must be resolved in order to clarify the applicable framework.²⁴ The regulations relative to real-estate agents (Art. 2 §3 of the Regulation) and to diamond traders (Art. 9 §2 of the Regulation) refer to tools and procedures developed in co-operation with professionals of the sector and approved by the Belgian authorities for the customer acceptance policy, and the use of which creates a presumption of compliance with legislative provisions. Owing to the complexity of the proposed decision processes, the expected 'appropriate use' (Art. 2 §3 for real-estate agents) or 'correct use' (Art. 9 §2 for diamond traders) should be defined to make the regulatory provisions applicable.

a5.102. **Criterion 22.2** – Art. 13 and 15 of the AML/CFT Law which govern record-keeping (see R 11) are applicable to non-financial businesses and professions. Notaries, accounting/tax professionals and diamond traders are also considering the possibility granted by Art. 38 §2 sub-para. 2 of the law of to keep the references of records in such a way that ensures they will be immediately able to produce the documents on request by the competent authorities, without the possibility that they have been altered or modified.

a5.103. **Criterion 22.3** – The shortcomings detected in respect of Art.12 of the law governing the due diligence measures to be taken in respect of PEPs are also found in the regulatory measures taken by the various professions (see R 12). The regulatory measures applicable to real-estate agents have already introduced the new requirements of R 12. There is some doubt as to the applicability of this approach as the definitions do not correspond to those contained in the law.

a5.104. **Criterion 22.4** – The law does not contain any measures concerning risk assessments to be carried out, in connection with the launch of products, business practices and new delivery means involving new technologies, even though, in practice, this assessment may be done under the general requirement to develop a risk-based customer acceptance policy, and to take enhanced measures where the transaction is carried out or the business relationship initiated remotely (see R 15).

a5.105. **Criterion 22.5** – The shortcomings noted for R 17 are found again in the measures applicable to non-financial businesses and professions, particularly with respect to reliance on institutions and persons established in an equivalent third country (see C.17. 2).

Weighting and conclusion

a5.106. Company service providers are not covered by the Belgian AML/CFT system. This sector was identified as at risk, in particular domiciliation companies, and measures are therefore being developed to require licensing and compliance with AML/CFT preventive measures. There are as well shortcomings as regards the customer due diligence requirements (R 10), which are one of the key components of R 22. There are also weaknesses for R 11, R 12, R 15 and R 17 which are not, however, specific to DNFBDs. In addition, the shortcomings relative to R 17 on reliance on third parties have a more minor impact regarding the activities of DNFBDs. **Belgium is largely compliant with R 22.**

Recommendation 23 – DNFBDs: other measures

a5.107. Belgium was rated largely compliant in the third evaluation (para. 623ff. MER 2005). The problem identified concerned the absence of requirements for legal and accounting professions to prepare written reports on transactions involving persons resident of non-cooperative countries when such transactions have no apparent economic or lawful basis.

a5.108. **Criterion 23.1** – The law requires non-financial businesses and professions to report suspicious transactions to the CTIF, with certain adaptations in relation to financial institutions (Art. 23 to 25).

24 Identification of the customer *or* the agent (Art. 3 §1 and §2, and 4 §3 of the Regulation of 4 October 2013); impossibility of performing 'certain' occasional transactions if the due diligence requirement could not be established (Art. 3 §3); taking of reasonable measures 'where possible' to verify the identity of the beneficial owners (Art. 5 §1).

PREVENTIVE MEASURES

a5.109. **Criterion 23.2** – The provisions of the law concerning internal controls and staff training and awareness also apply to non-financial businesses and professions, with some adaptations possible for appointing an AML/CFT officer, depending on the size of the organisation (Art. 18 para. 2). The regulatory measures on internal controls for lawyers, bailiffs, notaries and accounting/tax professionals introduce criteria for determining the size of the organisation that requires an AML/CFT officer. They also specify measures concerning training of personnel, and the integrity of personnel based on the risks involved in the tasks and duties to be performed. However, there is no independent audit function to test the AML/CFT system for any of the non-financial businesses and professions covered. Furthermore, the legislative provisions on AML/CFT programmes for groups (C.18.2) only apply to financial groups and do not apply to DNFBPs.

a5.110. **Criterion 23.3** – CTIF information on higher-risk countries is accessible to non-financial businesses and professions. The limits noted in respect of the framework in place (see R 19) are also found in respect of non-financial businesses and professions.

a5.111. **Criterion 23.4** – Art. 30 and 32 of the law apply to DNFBPs, with an adaptation for lawyers insofar as the president of the bar is responsible for reporting suspicious transactions. These provisions are repeated in the regulatory texts.

Weighting and conclusion

a5.112. The size of organisations for which there is no requirement to create an audit function reduces the impact of this shortcoming. **Belgium is largely compliant with R 23.**

Bibliography

BNB (nd a), *Listes, Établissements de crédit*, BNB, www.BNB.be/pub/cp/domains/ki/li.htm?l=fr

BNB (nd b), *Listes, Établissements de paiements et de monnaie électronique*, BNB, www.bnb.be/pub/cp/domains/psd/li.htm?l=fr

BNB (nd c), *Listes, Établissements de paiements agréés en Belgique*, BNB, www.BNB.be/pub/cp/domains/psd/li/psd1_li.htm?l=fr&id=psd1;%20

BNB (nd d), *Listes, Établissements de monnaie électronique agréés en Belgique*, BNB, www.BNB.be/pub/cp/domains/psd/li/em1_li.htm?l=fr&id=em1.

Chamber of Representatives (2009), *Projet de loi modifiant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et le Code des sociétés 2008-2009*, DOC 52 1988/001, www.lachambre.be/FLWB/pdf/52/1988/52K1988001.pdf

FATF (2005), *Third Round Mutual Evaluation Report of Belgium*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Belgium%20full%20FRE.pdf

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, www.fatf-gafi.org/recommendations

6. SUPERVISION

Recommendation 26 – Regulation and supervision of financial institutions

a6.1. Belgium was rated partially compliant in the third evaluation (para. 518 to 544, 553ff. MER 2005). The shortcomings were mainly due to the lack of resources for effective AML/CFT supervision in the insurance sector, to a lack of supervision of credit card issuers or managers (other than credit institutions), leasing and consumer credit companies, and to a doubt as to whether mortgage credit services were really supervised. At the time, the CTIF was the supervisory authority of these financial institutions, and it did not appear to have sufficient resources to perform this mission.

a6.2. **Criterion 26.1** – The scope of the AML/CFT Law includes all the financial institutions covered by the FATF Glossary. The 2010 overhaul of the structure of financial sector supervision entailed a new allocation of responsibilities, now shared by the BNB and the FSMA.¹ Given that AML/CFT supervision is integrated into prudential supervision, the BNB and the FSMA are respectively responsible for the AML/CFT supervision and regulation of institutions placed under their prudential responsibility. Consumer credit and leasing companies are supervised by FPS Economy.² The law expands its scope of application to the BNB and to the *Caisse des Dépôts et Consignations* in order to create a complete and effective AML/CFT framework. These two institutions are under the authority of the Finance Minister. Bpost is subject to the AML/CFT Law for its financial activities for own account (e.g. remittances/postal money orders, issuance of prepaid cards), and is under the supervisory control of FPS Finance. However, concerning activities performed as an agent of a credit institution or a European payment institution, it is not itself subject to the AML/CFT requirements; the institutions themselves are subject. As an agent, Bpost also acts as a ‘central contact point’ under the supervision of FPS Finance which oversees the European payment institution providing its activities in Belgium via the network of post offices (see R 14).

a6.3. **Criterion 26.2** – All of the institutions subject to the Core Principles are licensed by the BNB, including institutions authorised to perform money or value transfers (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).

a6.4. **Criterion 26.3** – For all financial institutions, legislative provisions require information to be provided about the capacity and professional standing of senior executives, when applying for licensing or registration.³ 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 to 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

1 See Section 6.1 of the main report.

2 The law of 31 July 2013 removed the provision of the law of 2 August 2002 which entrusted the FSMA with the task of supervising consumer credit companies and transactions, as of an effective date to be set by royal decree. It was decided that FPS Economy would be responsible for supervising credit regulation (mortgage and consumer credit) and that the FSMA would be responsible for supervising access to the business of lenders and intermediaries in these sectors. This distribution of responsibilities was given effect by the law of 19 April 2014. The section of that law on the FSMA’s responsibilities will come into force on 1 July 2015. Therefore, consumer credit is currently supervised by FPS Economy.

3 Particularly Art. 19 and 20 of the law of 25 April 2014; Art. 8 and 90 of the law of 9 July 1975; Art. 59 to 61 of the law of 6 April 1995; Art. 62 of the law of 21 December 2009.

SUPERVISION

of these financial institutions.⁴ The supervisory authority may deny a license or registration if it considers that the persons in question do not have 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 does not have 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 for prior notifications, thus giving the supervisory authority ongoing knowledge of the shareholding structure.

a6.5. **Criterion 26.4** – The AML/CFT Law provides that supervisory authorities responsible for financial institutions that are subject to AML/CFT requirements ‘may’ exercise their authority on a risk-sensitive basis (Art. 39 §1 sub-para. 2). The general supervisory framework in force in Belgium nonetheless provides that responsible authorities 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 on a risk-based approach. AML/CFT supervision, including the application of consolidated supervision of the group, is carried out within the framework of global oversight of financial institutions but may be supplemented by specific AML/CFT compliance inspections. b) For the other financial institutions, the FSMA states that it applies a risk-based supervisory approach. FPS Finance and FPS Economy did not provide any information about the method of supervision applied to Bpost or planned for consumer credit and leasing companies. Financial institutions offering MVTs or bureau de change services are subject to AML/CFT regulation and supervision (see R 14).

a6.6. **Criterion 26.5** – For financial institutions subject to their supervision, the BNB and the FSMA have introduced tools and processes to enable them to precisely define the institutions’ prudential risk profile and to identify the prudential supervision priorities, individually for each institution, and for the various sectors for which they are responsible. These elements particularly take into account the institution’s importance for the sector, its internal control procedures, its structure, the type of business it carries out, the profile of its customers and the characteristics of the products it offers. The ML/TF risk is one of the components taken into account to define the institution’s prudential risk profile, but the weight of the ML/TF risk identified for each institution is not sufficiently established for the BNB. The frequency and extent of inspections are therefore defined according to an approach based on the prudential risks to which the financial institutions are exposed. For the FSMA, ML/TF risk matrices have been defined, at least for the sectors to be supervised, and the ML/TF risk is therefore assessed but, except for bureaux de change, the impact on the frequency and extent of inspections to be carried out is not clearly established.

a6.7. **Criterion 26.6** – The BNB and the FSMA regularly review the risk profiles of the institutions they supervise, but the extent to which the ML/TF risk influences this revision is not established. They specify that the frequency of the profile review may depend on the way an institution’s risk profile changes, including in response to significant events or developments in the institution’s management and operations.

Weighting and conclusion

a6.8. The shortcomings relative to the assessment of ML/TF risk and on-site and remote inspection based on these risks have an important impact on the rating. **Belgium is partially compliant with R 26.**

A6

4 Art. 18 and 46 to 54 of the law of 25 April 2014; Art. 67 and 67bis of the law of 6 April 1995; Art. 207 and 208 of the law of 3 August 2012; Art. 23 and 24 of the law of 9 July 1975.

Recommendation 27 – Powers of supervisors

a6.9. Belgium was rated largely compliant in the third evaluation (para. 553ff. MER 2005). The main difficulty related to the lack of effective CTIF supervision of credit card issuers or managers (other than credit institutions), leasing companies and consumer credit companies.

a6.10. **Criterion 27.1** – The BNB and the FSMA have general powers to supervise or monitor financial institutions.⁵ The AML/CFT Law also grants them specific powers, to impose administrative sanctions for example, such as publishing the decisions made and/or imposing an administrative fine of at least EUR 250 and up to EUR 1 250 000 (Art. 40).

a6.11. **Criterion 27.2** – The AML/CFT Law grants supervisory authorities power to conduct on-site inspections (Art. 39 §2 sub-para. 2).

a6.12. **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 (Art. 39 §2 sub-para. 1).

a6.13. **Criterion 27.4** – The range of sanctions made available by the AML/CFT Law appears to be limited, insofar as it only includes publication measures and administrative fines (Art. 40). It does however appear to be satisfactory for financial institutions under BNB and FSMA supervision, as the latter may use the restrictive measures they have within the broader framework of their prudential sanctioning powers.⁶

Weighting and conclusion

a6.14. The shortcomings in terms of sanctions concern FPS Finance and FPS Economy. While FPS Economy is not involved in high-risk operations, FPS Finance is responsible for supervising a major European payment institution that is subject to AML/CFT requirements for the money transfer service it provides in Belgium via Bpost (agent and central contract point). **Belgium is largely compliant with R 27.**

Recommendation 28 – Regulation and supervision of DNFBPs

a6.15. Belgium was rated partially compliant in the third evaluation (para. 674ff. MER 2005). The implementation of the AML/CFT Law had not been defined for non-financial professions, and the systems for monitoring and supervising the obligations incumbent upon those professions were not in place, except for casinos. Furthermore, the structures responsible for compliance controls appeared to be lacking resources.

a6.16. Art.21 para. 1 of the AML/CFT Law lays down a general prohibition whereby merchants and service providers must not accept cash payments for goods or services worth EUR 3 000 or more, for an amount of more than 10% of the purchase price, provided it does not exceed EUR 3 000. This limitation on cash payment is important in the Belgian system, since the use of cash is identified as a factor of risk and vulnerability in the country. FPS Economy is responsible for detecting failures to comply with this provision. Following the analysis of the ML/TF threat, one or more sectors particularly at risk could be required, by RD, to inform the CTIF of any non-compliance with the limitation imposed (Art. 21 para. 5).

a6.17. **Criterion 28.1** – a) The Belgian Gaming Commission, which is an authority governed by the FPS 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 the physical casino. Foreign online casinos must

5 For example, Art. 134 of the law of 25 April 2014; Art. 92 §1 of the law of 6 April 1995; Art. 34 of the law of 2 August 2002.

6 See for example Art. 234 §1 of the law of 25 April 2014; Art. 104 §1 of the law of 6 April 1995; Art. 26 §1 of the law of 9 July 1975.

SUPERVISION

hold a licence in Belgium and the Gaming Commission 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)* The Gaming Commission is also responsible for the AML/CFT inspections of casinos, on the basis of the requirements of the AML/CFT law, the RD of 6 May 1999⁷ and the law of 7 May 1999.⁸

a6.18. **Criterion 28.2** – An authority responsible for monitoring compliance with AML/CFT requirements has been appointed for all other non-financial businesses and professions covered by the Belgian AML/CFT system. This is the FPS Economy for real-estate agents and diamond traders, and the FPS Interior for firms providing security services. The authorities responsible for monitoring legal and accounting/tax professions are public law institutions empowered to organise and supervise the profession by law.

a6.19. **Criterion 28.3** – All designated non-financial businesses and professions have defined regulatory measures establishing the principle of AML/CFT implementation oversight. The measures applicable to casinos have however been adopted in a broader framework than ML/TF prevention (see C.28.1 and R 22). Company service providers are not covered by the AML/CFT Law (see R 22).

a6.20. **Criterion 28.4** – *a)* The law grants all AML/CFT supervisory authorities general powers to seek disclosure of information and to conduct on-site inspections (except for independent legal professions and accounting/tax professions which have these powers nonetheless by virtue of their specific professional rules) to perform their supervisory mission (Art. 39 §2). *b)* All the professions lay down conditions of integrity and standing of natural persons for access to the profession, except for diamond traders. There are no rules governing supervision of shareholders or interests held in real-estate agencies or the diamond trade. For bailiffs, notaries and lawyers, only authorised professionals who have met the conditions of standing and integrity may manage and administer a firm or office. Among accounting/tax professions, registered auditors and chartered accountants and tax advisors require audit offices and/or statutory auditors to monitor companies and firms, both as regards shareholding and governing bodies. Certified accountants and tax advisors impose extensive monitoring requirements in respect of shareholders and the influence exercised in legal entities, both when an application is made to join the profession and throughout the company's existence. *c)* Without prejudice to the measures defined by other laws or regulations applicable to AML/CFT supervisors, Art.40 of the AML/CFT Law empowers them to impose administrative sanctions. The range of administrative sanctions provided by the law only includes publication measures and fines. However, there are also disciplinary sanctions applicable in each profession and business sector. The law does not establish any connection between the non-compliance detected and the applicable sanction, but the supervisory authorities may adjust the fine to the seriousness of the offences and use the range of sanctions available to them. Given the lack of indications concerning the sanctions policy, their proportional nature is difficult to assess.

a6.21. **Criterion 28.5** – The AML/CFT Law provides that authorities responsible for monitoring compliance with AML/CFT requirements 'may' exercise their control on a risk-sensitive basis (Art. 39 §1 sub-para. 2). Real-estate agents, companies providing security services and notaries state that they take the risk into account to determine their inspections, without giving any further details. The monitoring criteria established by diamond traders, and chartered accountants and tax accountants to a certain degree, are mainly based on the existence and quality of the annual AML/CFT report, which is used to determine inspection priorities for professionals. For the other professions and businesses, monitoring programmes have been established without any individual professional risk assessment (e.g. company auditors), and without any reference to

A6

7 RD implementing Art. 14bis §2 sub-para. 2 of the AML/CFT Law which defines a list of objective criteria in order to make targeted declarations.

8 Law on gaming, gaming houses and the protection of gamblers which contains provisions relative to the identification requirement (see R 22).

the sector's overall risk. No indication is provided of how the risk profile of covered institutions impacts the scope and frequency of inspections.

Weighting and conclusion

a6.22. There are several shortcomings: the absence of fit-and-proper requirements affects in particular the diamond trade sector, which is recognised as high risk. In addition, the shortcomings noted in respect of the basic principles on which AML/CFT inspections are defined and the failure to take ML/TF risks into account in the approach developed by all DNFBPs heavily influence the rating. **Belgium is partially compliant with R 28.**

Recommendation 34 – Guidance and feedback

a6.23. Belgium was rated largely compliant in the third evaluation (former R 25, para. 545ff. MER 2005). The FATF underlined the lack of guidance, particularly with regard to non-financial professions. The new R 34 of 2012 extends the obligation to supervisors and self-regulatory bodies.

a6.24. **Criterion 34.1 – Guidelines:** On its website, the CTIF publishes general and topic-specific educational AML/CFT information (particularly relating to asset freezing obligations), and draws up guidelines for relevant professionals and institutions. It also maintains relations with reporting entities particularly by taking part in training seminars. Its annual reports help relevant entities to understand AML/CFT provisions. FPS Finance (Treasury Administration) publishes information about sanctions, embargoes and cash transfers.

a6.25. The BNB and the FSMA issue circulars and updates, including commentaries, for financial institutions under their supervision, to give them a complete, systematic and coherent view of legal and regulatory AML/CFT requirements (including European requirements). They also state their expectations as regards the implementation of these requirements. When necessary, common circulars are issued. FPS Finance and FPS Economy have not prepared any guidance for the companies they supervise.

a6.26. Most authorities responsible for AML/CFT supervision of DNFBPs have provided guidance on the applicable AML/CFT provisions by means of circulars, guides and memos designed to explain the applicable AML/CFT measures and facilitate application. However, no specific measure appears to have been taken recently for companies providing security services, casinos, lawyers of French-speaking and German-speaking Bar associations, and bailiffs.

a6.27. *Feedback:* The CTIF states that it conducts a quality review of the reports received from each sector or from a given entity in particular, although this procedure is not formalised or systematic and does not correspond to regularly organised exchanges. In addition, the CTIF contributes through its strategic analysis section to a better understanding of ML/TF trends, an analysis that allows the indicators and suspicions of reporting institutions to be placed in context. Overall feedback about reports received is provided in the annual report, through statistics specific to each reporting sector and the typologies presented. The CTIF analysts are in contact with compliance officers: Requests for additional information in connexion with STRs can also contribute to improving future reporting when they indicate an omission or lack of clarity. These various levels of examination can lead to informing a supervisory or disciplinary authority of the findings made in respect of professionals under its responsibility. Supervisory authorities do not take part in or initiate any sectoral feedback. Such actions could help reporting entities detect and report suspicious transactions.

Weighting and conclusion

a6.28. SPF Finance and SPF Economy, as well as the oversight authorities for casinos, the French- and German-speaking bar associations and bailiffs have not produced any specific AML/CFT guidelines recently. Supervisors do not participate in, nor do they take the initiative in providing sectoral feedback in relation to the implementation of reporting obligations, on the basis of observations made during their inspections. Such actions might help reporters detect and report suspicious transactions. **Belgium is largely compliant with R 34.**

A6

Recommendation 35 – Sanctions

a6.29. Belgium was rated largely compliant in the third evaluation (para. 492ff. MER 2005), but the proportionality of the sanctions was not closely examined. The difficulty identified concerned the effectiveness of sanctions for certain financial institutions (credit card issuers and managers other than credit institutions, and leasing and consumer credit companies).

a6.30. **Criterion 35.1** – The AML/CFT Law makes provision for administrative sanctions for failures to meet due diligence, record-keeping, internal organisation, suspicious transaction reporting and communication of information requirements by all organisations subject to it (Art. 40). These sanctions may also be applied in respect of any violations of financial embargo obligations (R 6) laid down by EU Regulations,⁹ where they involve failures to comply with requirements to inform the CTIF of transactions suspected of being related to terrorist financing, and shortcomings in the organisation and internal control required to ensure effective prevention of both TF and ML. Criminal sanctions for violations of the requirements of these Regulations are also provided for (Art. 6 of the law of 13 May 2003). They may be imposed against any natural or legal persons, including financial or non-financial institutions subject to the AML/CFT Law. The AML/CFT Law applies to covered institutions, without distinguishing natural from legal persons. Real-estate agents specify that AML requirements apply to them as natural persons. Notaries, bailiffs and lawyers are always personally liable, even if they work in the framework of a company. For the accounting/tax professions and companies providing security services, the legal entities and the natural persons responsible for the violations may be sanctioned. For the financial institutions under their supervision, the BNB and the FSMA may also use the measures they have in the more general framework of their prudential sanctioning powers (see C.27.4.). The range of sanctions is quite broad. To assess the proportionality of sanctions, it has not been established whether or not and how the scale or type of sanctions may vary depending on the nature and extent of the violation, the institution in violation (e.g. financial institution/non-financial profession, size and financial situation), the amount of the transaction in question to determine the amount of administrative sanctions, the severity and number of grounds, the case of repeated offences, or any other relevant criteria.

a6.31. **Criterion 35.2** – Where sanctions are imposed against legal persons, the senior executives may also be sanctioned. For some DNFBPs, a disciplinary sanction it is required. Regarding financial institutions supervised by the BNB and the FSMA, if the senior executives are directly involved in the violation for which their financial institution is sanctioned under Art.40 of the AML/CFT Law, their required standing and/or expertise may be challenged and the competent authorities may, depending on the seriousness of the offence, use the enforcement powers they have under these same prudential laws (see 26.3). These authorities may thus, *inter alia*, require the financial institutions in question to dismiss the relevant senior executives.¹⁰

Weighting and conclusion

a6.32. **Belgium is largely compliant with R 35.**

A6

⁹ Regulations 881/2002 (Al Qaeda), 2580/2001 (concerning certain persons and entities with a view to combating terrorism), 329/2007 (restrictive measures against the Democratic People's Republic of Korea) and 267/2012 (restrictive measures against Iran).

¹⁰ The Belgian authorities state that, when they transpose into Belgian law the 4th AML/CFT Directive currently being developed, they will examine the need to clarify the current provisions.

7. LEGAL PERSONS AND ARRANGEMENTS

Recommendation 24 – Transparency and beneficial owners of legal persons

a7.1. Belgium was considered in 2005 to be partially compliant with former R 33 due to a lack of transparency and insufficient supervision of bearer bonds (para. 719ff. MER 2005). The types of legal persons relevant to R 24 in Belgium are companies, foundations and associations (described in Section 7).

a7.2. **Criterion 24.1 – a)** Belgium has mechanisms for identifying and describing the various types, forms and features of entities which may be incorporated under Belgian law, including foundations and associations, and *b)* procedures for creating such entities and methods for obtaining and preserving basic information and that concerning their beneficial owners. Such information is made available to the public via several websites.¹

a7.3. **Criterion 24.2 –** Belgium has not assessed horizontally the ML/TF risks associated with different categories of legal persons formed therein. The national analysis of ML threat, risk and vulnerability nonetheless contains relevant information on the potential use of legal persons for criminal purposes (use of dormant, ‘shell’ and sham companies). The Federal Police also point to the vulnerability of SMEs, including *SPRLs* (due to the small amount of capital required for incorporation). Comparable information is also available, but less so concerning TF risks, especially for the NPO sector (see R 8). The authorities therefore have a certain amount of information on ML/TF risks associated with the categories of entities which may be incorporated in Belgium, even though such information could be collected in a more systematic and co-ordinated manner and certain information kept updated.

a7.4. **Criterion 24.3 –** Basic information concerning all types of legal person is kept in a filing with the registry of the Commercial Court within whose jurisdiction the company’s registered office is located. This information is also published in *Moniteur belge* (the official journal) and accessible via the BCE,² the Belgian companies register. The BCE database is available to the public with a search facility in French and Dutch.

a7.5. **Criterion 24.4 –** In Belgium, all companies limited by shares must keep a register (usually at the registered office) for each category of registered security it issues, including separate registers for shares and bonds (Art. 460 and s. *Code des sociétés* – Belgian company law). The name and number of shares in partnerships are included in their articles of association. Information concerning the holder(s) of dematerialised securities is kept by an approved account depository (see C.24.11). For associations, a register of members must be accessible at the association’s registered office (Art. 31, Belgian Law of 27 January 1921). A Belgian foundation has neither members nor shareholders, but the name of each founder must be included in its articles of association (Art. 27, Law of 27 January 1921).

a7.6. **Criterion 24.5 –** The provisions of AML legislation apply on creation of a legal person, for which act authenticated by a notary is required (*SA, SCRL, SPRL, SCA, AISBL* and foundations). The notary who prepares and verifies the articles of association must also verify the identity of the entity’s founders and any person lawfully holding shares in the company (Art. 7, AML/CFT Law). According to the risk involved, the notary is also obliged to keep the collected identification data updated. He also verifies and makes amendments to the articles of association and changes in the entity’s operation (registered office, legal status, identity of shareholders, founders, directors, etc.), excluding share transfers. Such documents must be filed in the registry of the Commercial Court and published in *Moniteur belge*, and are then accessible via the BCE. The Commercial Court registry carries out a formal check of the filed information for any legal person not created

1 For example www.belgium.be/fr/economie/entreprise/creation/types_de_societe/ or http://economie.fgov.be/fr/entreprises/vie_entreprise/Creer/#.Uue7IE01jJ4.

2 <http://economie.fgov.be/fr/entreprises/bce/#.VFHg7fldVik>.

by a notary's authentic act.³ Ownership of securities is registered by their holder in the company register. Lack of such registration renders any transfer of securities unenforceable against third parties.

a7.7. **Criterion 24.6** – The information recorded in the share register or BCE mainly provides information on legal ownership of the entity which may match its beneficial ownership. Several mechanisms enable discovery of beneficial owners: 1) *use of existing information, including that obtained from financial institutions and non-financial professionals* such as notaries (Art. 8 AML/CFT Law), while noting that access to such information is dependent on the data provided by the client companies themselves. The introduction of a provision into the *Code des sociétés* extending the obligation to declare holdings of 25% or more in unlisted companies issuing dematerialised shares⁴ also enables relevant information to be obtained; 2) *use of any information available on listed Belgian companies*, including via the obligation to publish major holdings in a company under which the identity of holders of over 5% of the share capital is revealed (Law of 2 May 2007). Access to BCE also allows tracking of the ownership chain for entities registered in Belgium. Financial institutions and non-financial professionals are obliged to test such information for credibility and relevance (Art.8 §3 al.2). If the test proves positive, the financial institution or non-financial professional then verifies the identity of the beneficial owners taking appropriate measures adapted to the risk. If a financial institution or non-financial professional doubts the credibility and relevance of the information provided, it will take any other reasonable and appropriate measure to identify the customer's beneficial owners and verify such identities. There is no legal restriction on timely access to such information by the competent authorities when the evidence points to a breach of AML/CFT obligations.

a7.8. **Criterion 24.7** – The precise nature of beneficial owner information obtainable from covered professionals may be determined when the information is capable of being verified by official sources (see C.24.6 – authenticated act, declaration of major holdings, registers of listed companies, etc.). As for updating, legal persons are firstly obliged to provide the financial institutions and DNFBPs with which they have dealings with the identity of their beneficial owners and with an update of such information when requested. There is neither a time-limit for provision of updates nor penalty for failing to provide the information (apart from possible termination of the business relationship). Covered professionals are themselves obliged to update their customer identification data, according to risk (see R 10 and R 22). These professionals are secondly obliged to verify the 'credibility and relevance' of information provided to them by legal persons, i.e. that the information received complies with the law and that there is no inconsistency, element or factor which discredits the information provided and leads to doubts as to its veracity (see R 10).

a7.9. **Criterion 24.8** – Managers and directors of legal persons are obliged to provide complete basic data and available information about beneficial owners (without the need for specific authorisation in the case of companies) and to provide any other form of assistance to the competent authorities (Art. 527, Companies Code on the general liability of managers and directors). Such information must be accessible at the company's registered office, i.e. in Belgium, even though there is no condition of residence for a representative in the Companies Code.

a7.10. **Criterion 24.9** – The file for each legal person is kept for 30 years at the registry of the Commercial Court and the BCE. 'Paper' files are then transferred to the royal archives (*Archives générales du Royaume*). Information relating to customer identification is kept by the financial institutions and non-financial professions in compliance with the FATF standard (see R 11 and R 22). Data in the share register is kept

3 The court registry is not permitted to verify the lawfulness of clauses in the articles of association or the content of minutes of general meetings or the board of directors. The possibility of extending the supervisory powers of court registries to ID data for managers/directors representing legal persons is under discussion.

4 However, the declaration received by the company pursuant to Art. 515bis, Company Code, may only be a starting point in certain cases enabling the company concerned to concentrate on declarations of holdings exceeding 25% in its research for information to be provided to due diligence professionals. This would be the case where a declaration to the client company is made by a corporate shareholder. These declarations supplement existing sources of information. In seeking the identity of its beneficiaries, the client company may also thereby refer, for example, to the register of shareholders or lists of attendees at its general meetings.

throughout the entity's lifespan. Actions against legal persons are time-barred after 5 years; the documents must therefore be kept for 5 years after winding-up (Art. 198, Companies Code, and art. 25 and 41 of the Law of 27 June 1921 for associations and foundations).

a7.11. **Criterion 24.10** – Competent authorities and especially law enforcement authorities have the necessary powers to obtain access to information kept by companies and other legal persons, including that kept in the registers (see R 31). There is no legal or regulatory restriction on timely access to basic and/or beneficial owner information by these authorities when the evidence points to a breach of AML/CFT obligations.

a7.12. **Criterion 24.11** – The Law of 14 December 2005 on the elimination of bearer bonds was brought into force in stages and became fully applicable on 1 January 2014. The identity of Belgian shareholders is now known, due to a dual system: (i) the registered share system, enabling a company to identify its shareholders as it must now keep a share register; (ii) the dematerialised share system under which the identity of a holder of securities is known to the account depository.⁵ The concept of 'securities' in the 2005 law extends to share subscription rights (Art. 2 1°).

a7.13. **Criterion 24.12** – Certification of shares⁶ in Belgium is similar to 'nominee shareholding' in terms of legal structure although its objectives and certain features differ. Under Art. 503 §1er, al. 3, Companies Code, the issuer of certificates relating to registered shares must make its status known to the company which issued the certified shares, which enters such status in the register concerned, before any exercise of voting rights if the certificates relate to dematerialised securities. Unless otherwise provided, the certificate issuer may not transfer the securities associated with the certificates. No transfer of securities associated with the certificates may be made if the issuer has made a public offering (Art. 503, §1^{er}, al. 5).

a7.14. Belgium also allows *directors* to act on behalf of others ('nominee director'). If such directors are legal persons, they must appoint a permanent representative to carry out their duties for and on behalf of the legal person (Art. 61 §2, Companies Code). The identity of the director must be filed at the Commercial Court registry, published in *Moniteur belge*, registered with the BCE and appear in the company register. Appointment and removal of the permanent representative are only subject to the same publication rules as if he exercised these duties on his own behalf.

a7.15. Shares in Belgium may also be registered in the name of a nominee ('nominee subscription'). This arrangement is based on a nominee agreement (Art. 7 §2) of which the financial institution must be informed as part of its due diligence obligation. The nominee's identity is verified from information kept in the register of shareholders which refers to the nominee agreement (Art. 7 §2, AML/CFT). However, the identity of the real shareholder (which might be a foreign company) does not appear in public registers or in the company's register. Neither the status of the nominee nor its identity is disclosed. Such lack of publication hampers discovery of the identity of the shareholder. Nominee-held shares in Belgium are not therefore subject to sufficient measures to ensure that their use not is being abused.

a7.16. **Criterion 24.13** – Any legal person which has not filed the full text of its Art. of Association in the registry of the Commercial Court within three months of the date of the acts is subject to a fine of between EUR 50 and EUR 10 000 (Art. 90 and 91, Companies Code). Moreover, unregistered companies do not acquire legal personality. Absence of or delay in filing with the Commercial Court registry incurs a fine of between EUR 25 and EUR 250 per month's delay (Art. 256(1) *Code des droits d'enregistrement, d'hypothèque et de greffe*). The Law of 16 January 2003 establishing the BCE also imposes administrative and criminal sanctions for non-compliance with its provisions, especially its registration obligations (Art. 62 §2 and 5, and art. 63).

5 As from 1 January 2014, the law provides that remaining bearer securities will be automatically converted to dematerialised securities and registered in the share register, unless the issuer (the company) decides to convert them to registered securities and register them in its name. Finally, if the holder of the securities is still unknown on 1 January 2015, the securities concerned will be sold by the issuer.

6 See Section 7.1 (b).

LEGAL PERSONS AND ARRANGEMENTS

Company directors are liable to their companies and third parties for prejudice caused by breach of the company's Articles of Association and for mismanagement by failing to keep share registers of *SAs* and *SCAs* or of *SPRLs*, *SCRLs*, *SCRIs* (Art. 263, 408, 528 and 657, Companies Code). Case law expressly provides that a company which fails to fulfil its legal obligation to keep a share register is liable to any shareholder prejudiced thereby. The Companies Code also imposes criminal sanctions in the event of deliberately erroneous or misleading entries in share registers (Art. 348, 388 and 649): imprisonment for between one month and three years and a fine of EUR 26 to EUR 3 000 (Art. 496 PC). The sanctions contained in the Penal Code also apply to partnerships. Sanctions also apply in relation to obligations dealing with non-listed companies (Art. 516). Nullity of an association (and therefore its liquidation) or of a foundation may be declared if the Articles of Association do not contain required legal clauses. Legal persons (or their representatives) are not liable to penalties for simply having passed on erroneous or misleading information about their beneficiaries to professions subject to due diligence when such information is provided by their beneficial owners (Art. 8, AML/CFT Law), but the consequences of such acts may incur sanctions. The lack of information concerning sanction policy hampers assessment of the proportionality of punishment.

a7.17. **Criterion 24.14** – The competent authorities have measures for international co-operation and investigative powers which may be used to exchange information about companies, shareholders and beneficial owners. Directive 2012/17/EU on the interconnection of central, commercial and company registers, which Belgium is in the process of implementing, should improve access to such information. An analysis of R 37 and R 40 does not disclose any particular obstacle liable to impede this type of exchange of information. No legal or regulatory provision prevents swift transmission of such information to foreign competent authorities.

a7.18. **Criterion 24.15** – For international criminal mutual assistance, Belgium has mechanisms to assess the quality of information it obtains (by the investigating judge who initiated the request and each public prosecutor's department) enabling discovery of any structural problem in co-operation with another country. Besides the judicial mechanisms, the CTIF has tools and resources enabling supervision and control of the quality of international co-operation.

Weighting and conclusion

a7.19. **Belgium is largely compliant with R 24.**

Recommendation 25 – Transparency and beneficial owners of legal arrangements

a7.20. In 2005, it was considered that the FATF standard dealing with the transparency of legal arrangements did not apply to Belgium as it had no such structures (former R 34). The changes made in R 25 provide that the country must apply minimum transparency requirements even if it does not legally recognise trusts. R 25 therefore now applies to Belgium, even though an *express trust*, as known to the English-speaking world, cannot be created in Belgium (see Section 7 of the main report).

a7.21. **Criterion 25.1** – The requirements set out in a) and b) do not apply to Belgium. c) Financial and non-financial professions whose customers are legal arrangements are subject to obligations of identifying their representatives and beneficial owners, verifying the identity of the latter and keeping all collected data for 5 years (Art. 7, 8 and 13, AML/CFT law). Pursuant to the general rules of tax law, professional trustees are also obliged to keep all information enabling determination of their income, including information concerning the trusts they administer.⁷

a7.22. **Criterion 25.2** – The professions approved to act in Belgium as professional *trustees* are covered professions (notaries - Art. 3.1, AML/CFT law, accountancy professionals – Art. 3.4, lawyers - Art. 3.5 a) 5) are obliged to update, according to risk and whenever they are advised that their data is no longer up-to-date, customer identification data, including any related to trusts and fiduciary or other legal arrangements

A7

⁷ Global Forum, Peer review report: Phase 2, practical implementation of standards, Belgium, 2013.

(see C.24.7). This includes information on beneficial owners, initially subject to ‘credibility and relevance’ verification (Art. 8 §3 and §2) (see R 10 and R 22). However, updating on the basis of risk does not establish that the information is updated promptly and kept as up-to-date as possible.

a7.23. **Criterion 25.3** – The AML/CFT Law requires the identification and verification, via supporting documents, of the identity of the customer’s representatives, i.e. persons acting in any capacity for and on the customer’s behalf (Art. 7 §2). Legal arrangements are also obliged to provide information concerning their beneficial owners to financial and non-financial professions with which they have a business relationship or with whom they transact on an ad hoc basis (Art. 8 §3).

a7.24. **Criterion 25.4** – No legal or regulatory provision prevents professional *trustees* from communicating information concerning a legal arrangements to the competent authorities or professions subject to due diligence.

a7.25. **Criterion 25.5** – Competent authorities and especially prosecution authorities have the necessary powers to obtain access to information kept by trustees, including covered professions (see R 31). Moreover, as from the 2013 tax year, the tax authorities hold information from the tax return of physical persons who are founders, beneficial owners or potential beneficial owners of legal arrangements, including foreign ones.⁸ There is no legal or regulatory obstacle to the competent authorities having prompt access to this information.

a7.26. **Criterion 25.6** – The competent authorities have measures for international co-operation and investigative powers which may be used to exchange information about trusts. An analysis of R 37 and R 40 does not disclose any particular obstacle liable to impede this type of exchange of information. No legal or regulatory provision prevents swift access of such information by foreign competent authorities.

a7.27. **Criteria 25.7** – Professions in Belgium acting as professional *trustees* and which are subject to the AML/CFT system are legally liable for any breach of their obligations.

a7.28. **Criterion 25.8** – The sanctions imposed by the AML/CFT Law for violations of the due diligence and record-keeping obligations apply to all covered professions, including professional *trustees* (Art. 40). There is no clear policy on applicable sanctions enabling determination of their proportionality. No legal or regulatory provision prevents swift access of such information by competent authorities.

Weighting and conclusion

a7.29. Due to the limited development of trusts and legal arrangements in Belgium, the obligations of R 25 apply principally to professional *trustees* which are generally subject to the AML/CFT obligations. The activities of non-professional trustees not covered by AML/CFT obligations are not significant. **Belgium is largely compliant with R 25.**

8 Art. 307 para. 1 sub-para. 4, Income Tax Code, as amended by the Law of 30 July 2013 introduces an obligation for Belgian taxpayers to declare any legal arrangement of which they (or their spouses and children) are founders, beneficiaries or potential beneficiaries. This covers trusts, fiduciary structures and foreign structures which are either subject to no or low tax, a list of which was established by Royal Application Decree of 19 March 2014.



8. INTERNATIONAL COOPERATION

Recommendation 36 – International instruments

a8.1. In 2005, Belgium was assessed as largely compliant with the FATF standard on international instruments as concerns AML/CFT (former R 35 and SR I; Section 6.2, MER 2005) because there were doubts remaining over full transposition of certain treaties on declaring cross-border cash movements and the definition of funds to be frozen in application of UNSCRs, matters on which progress has been made (see R 32 and R 6).

a8.2. **Criterion 36.1** – Belgium is a Party to the Conventions of Vienna (since 1996), Palermo (since 2004), Mérida (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).

a8.3. **Criterion 36.2** – Belgium has reinforced its compliance with the provisions of the Conventions of Vienna, Palermo and that on TF, and has fully implemented the Merida Convention.

Weighting and conclusion

a8.4. **Belgium is compliant with R 36.**

Recommendation 37 – Mutual legal assistance

a8.5. In 2005, Belgium was assessed as largely compliant with the FATF standard on mutual legal assistance (former R 37 and SR V) due to a relative effectiveness for assistance outside the framework of bilateral agreements and a lack of statistics (Section 6.3, MER 2005). The first point was resolved by the Law of 9 December 2004 (whose effectiveness could not be evaluated in 2005), but the second remains problematic.

a8.6. **Criterion 37.1** – Belgium may provide legal assistance to other countries under bilateral and multilateral conventions it has ratified and may provide as much legal assistance as possible in criminal matters, subject to the law and applicable international law (see MER 2005 for a list of treaties). The Law of 9 December 2004 on international legal assistance in criminal matters also governs enforcement in Belgium of requests for assistance from States with which Belgium is not internationally linked by a convention on mutual legal assistance, on the basis of reciprocity.

a8.7. **Criterion 37.2** – SPF Justice is the central authority in the area of international co-operation in criminal matters for requests concerning countries outside the EU; requests from within the EU are sent directly to the judicial authorities and SPF Justice advised accordingly. Within the prosecution authority, the federal prosecutor's office is empowered to manage any type of outgoing or incoming request for international co-operation in criminal matters. Transmission of the letters rogatory is made either directly from one judicial authority to another in a country with which Belgium is linked by an international convention, or after being authorised by the Minister of Justice in other cases.¹ The federal prosecutor's office facilitates execution of requests for legal assistance, whatever the offence concerned. It is also the central point of contact 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 it has a request registration system, operational since 1 January 2004. However, the registration system does not enable supervision or checking of the due execution of either outgoing or incoming letters rogatory, or measuring the time taken for execution and

1 Circular no COL 5/2005 of the College of Prosecutors-General and the Ministry of Justice contains instructions for dispatch and receipt of requests for assistance to and from judicial authorities.

INTERNATIONAL COOPERATION

cannot therefore be regarded as a management system. It is not integrated, i.e. it is not accessible to the Kingdom's courts or judges. The central authority has therefore no automatic system for following up on requests whose execution is delayed, but can only react to reminders from the requesting authority. There are no formal criteria for managing request urgency or for establishing priorities and prompt execution of requests for judicial assistance. The system does not enable collection of statistical data on assistance activity.

a8.8. **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 no reciprocity commitment, or if execution might harm sovereignty, security, public policy or other 'essential interests of Belgium' (undefined, but according to the Belgian authorities this ground has never been the basis for non-execution of a request for assistance in the field of economic and financial criminality). 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 the rule in principle is to honour requests for assistance.

a8.9. **Criterion 37.4** – Since entry into force of the Law of 9 December 2004, 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).

a8.10. **Criterion 37.5** – Bilateral conventions with Belgium provide as a general rule that the requested State and the requesting State 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 execution. This immediately involves investigative and examining secrecy and thereby the confidentiality of the foreign request for assistance.

a8.11. **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, dual criminality does not apply to requests for mutual legal assistance in the case of non-coercive measures. Coercive measures are defined in the CPC as measures which 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).

a8.12. **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 a requirement of dual criminality (see C.5.2).

a8.13. **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

a8.14. Belgium lacks clear procedures for establishing the priority and execution of requests for judicial assistance. Moreover, the current file management system does not enable supervision or control of execution of letters of request. **Belgium is largely compliant with R 37.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

a8.15. The application of seizure and confiscation measures as part of mutual legal assistance was considered to be largely compliant with the FATF standard in 2005 due to the absence of a fund for the seized assets and an inability to share confiscated assets (former R 38; Section 6.3, MER 2005).

a8.16. **Criterion 38.1** – *System applicable to requests for assistance outside the EU.* Belgium adopted a law on 20 May 1997 on international co-operation for seizure and confiscation. Mutual legal assistance in this area is governed by the following general principles: (i) a system based on a convention prior to the request; (ii) the request may be refused on certain grounds, including when execution of the request might prejudice sovereignty, security, public policy or other basic interests of Belgium or if the request might prejudice investigations or prosecutions brought by the Belgian authorities.

a8.17. *System applicable to requests for assistance within the EU.* The Law of 5 August 2006 on the application of the principle of mutual recognition of judicial decisions in criminal matters between member states of the EU transposed framework decisions 2003/577/JAI and 2006/783/JAI into Belgian law. This law establishes a single framework for the execution of judicial decisions concerning assets. It sets out reasons for refusing execution of a request, including the absence of dual criminality. The fact that TF is not criminalised in Belgium in full compliance with the international standard may impede mutual assistance based on a requirement of dual criminality (see C.5.2).

a8.18. The ability to take expeditious action in response to a request for assistance concerning the identification of property liable to be seized and confiscated: Belgium is able to respond to such requests for assistance by giving ordinary assistance (see R 37). The OCSC now has wider powers to obtain information of this kind (Law of 11 February 2014) but it is uncertain as to how far these powers apply in responding to a request for assistance.

a8.19. The ability to take expeditious action in response to a request for assistance concerning a request for seizure: Measures for execution of foreign seizure decisions from non-Member States are set out in Chapter III of the Law of 20 May 1997. The law lists the request execution conditions (including dual criminality) and establishes the execution procedure. Procedurally, the judges in chambers (*en chambre du conseil*) of the first-instance court having jurisdiction over the area where the property is located must, before any seizure, make a decision of *exequatur*, when it considers whether the legal conditions have been fulfilled. Such order is made within 5 days of receipt of the request by the judge in chambers. In urgent cases, the investigating judge may order provisional execution of measures, provided the judge in chambers subsequently confirms the measures. The Law of 20 May 1997 requires an in chambers ruling both for obtaining *exequatur* and for authorising transmission of seized documents and goods. In a European context, the Law of 5 August 2006 provides that the competent authority is not SPF Justice but the Royal Prosecutor for the place where the property is located with a view to direct co-operation between the competent authorities, thereby facilitating and improving execution of requests for seizure. The investigating judge must rule on execution of the seizure, preferably within 24 hours and at the latest within 5 days of referral. The authorities state that the procedure provided in the Law of 20 May 1997 is intended to protect Belgian interests (a Belgian investigation concerning the same facts or persons) or those of third parties.

a8.20. The ability to take expeditious action in response to a request for assistance concerning a request for confiscation: Belgium treats requests for confiscation in the same way and within the same period as it treats domestic matters (see R 37).

a8.21. **Criterion 38.2** – Under Belgian criminal law, confiscation is a punishment dependent on a principal sentence of imprisonment or a fine. It is therefore impossible to impose a confiscation measure without a prior criminal conviction.

a8.22. **Criterion 38.3** – The Law of 26 March 2003 assigned OCSC to manage international mutual legal assistance for seizures, confiscation and execution of judgments and orders concerning assets linked with offences. OCSC is the authority responsible for the management of seized funds and has had its remit strengthened in this area (see R 4). OCSC is a member of the CARIN network and the designated *asset recovery office* in Belgium. This mechanism provides for an exchange of information between the different national offices of EU Member States, both spontaneously and upon request. Exchange is subject to the procedures in the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States, which has not yet been transposed into Belgian law. The authorities state that OCSC has not signed any agreement with its foreign counterparts.

INTERNATIONAL COOPERATION

a8.23. **Criterion 38.4** – Art.38 of the Law of 5 August 2006 established a rule for sharing confiscated assets. In the event of co-operation with a non-Member State, an asset division clause is provided in Art.8 of the Law of 20 May 1997.

Weighting and conclusion

a8.24. The general procedures for mutual legal assistance in criminal matters apply to identification and confiscation requests, with the same doubts concerning their expedited nature. **Belgium is largely compliant with R 38.**

Recommendation 39 - Extradition

a8.25. Belgium was considered to be largely compliant in 2005 with the FATF standard on extradition, due to the problematic and ineffective procedures for extradition outside the EU (former R 39; Section 6.4, MER 2005). Belgium co-operates with EU Member States by virtue of the European arrest warrant law of 19 December 2003, which came into force on 1 January 2004. Outside the EU, the ordinary principles of extradition apply pursuant to the Law of 15 March 1874, as amended first by the Law of 31 July 1985 and then by the Law of 15 May 2007, and the bilateral and multilateral agreements to which Belgium is a Party. There has been no major change to Belgian extradition legislation since this assessment.

a8.26. **Criterion 39.1** – a) ML and TF offences may give rise to extradition. b) Belgium has clear extradition procedures but which do not enable priorities to be set due to the lack of a request management tool (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, MER 2005). Moreover, the fact that TF is not criminalised in Belgium in full compliance with the international standard (see C.5.2) may hamper extradition. c) Execution of requests for extradition is not coupled with unreasonable or unduly restrictive grounds or conditions. In European cases, a Member State does not execute 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 1874 law requires the existence of a treaty between Belgium and the requesting State as a condition of any extradition. The conditions of the EU and Council of Europe treaties comply with the standard.

a8.27. **Criterion 39.2** – Belgium may extradite its nationals and residents in Belgian territory to an EU Member State under a European arrest warrant (if appropriate, on condition that the person concerned is returned to Belgium after conviction to serve his sentence). Outside the EU, Belgium does not extradite its nationals, but the Belgian authorities state that ‘in principle’ prosecution is undertaken if the requesting State is a party to the European Convention on Extradition or has signed a bilateral extradition agreement with Belgium. Belgium can therefore refuse extradition of its nationals (outside the EU) without undertaking to prosecute the conduct upon which the request is based. The refusal criteria are not governed by the law.

a8.28. **Criterion 39.3** – The 1874 law requires that the facts giving rise to extradition are punishable both under Belgian law and under the law of the requesting State. It does not however require that classification of the facts be the same in both countries. The Law of 19 December 2003 provides that a European arrest warrant may be executed without testing for dual criminality in a certain number of cases including ML and TF.

a8.29. **Criterion 39.4** – Belgium has simplified extradition mechanisms for executing the European arrest warrant, which then replace the traditional extradition system. Outside Europe, the extradition procedure is simplified if the person concerned consents to his extradition.

Weighting and conclusion

a8.30. The extradition procedures do not enable priorities to be established due to the absence of a request management tool and the extradition conditions outside the EU are cumbersome and complicated, which does not guarantee extradition without delay. The lack of criteria for prosecution or otherwise if extradition is refused is also a concern. **Belgium is largely compliant with R 39.**

Recommendation 40 – Autres formes de coopération internationale

a8.31. Belgium was considered to be largely compliant in 2005 with the FATF standard which set out other forms of international co-operation (apart from mutual legal assistance and extradition, former R 40; Section 6.5, MER 2005). The Recommendation was significantly modified in 2012.

a8.32. **Criterion 40.1** – The competent authorities in Belgium are able promptly to provide the widest possible range of international co-operation– both spontaneously and upon request – in the areas of ML, underlying predicate offences and TF.²

a8.33. **Criterion 40.2** – a) International co-operation has a legal foundation (see C.40.1). b) There is no impediment to use of the most effective means of co-operating. c) The CTIF and the Federal Police use clear and secure channels, circuits and mechanisms to facilitate transmission and execution of requests.³ d) The CTIF, AGDA and the Federal Police have clear procedures for establishing priorities and facilitating timely transmission and execution of requests. It has not been established 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).

a8.34. **Criterion 40.3** – The CTIF, police authorities, AGDA, BNB and FSMA have signed bilateral agreements, MoUs and protocols to facilitate co-operation with numerous foreign counterparts. There is no indication that these agreements were not signed in a timely manner.

a8.35. **Criterion 40.4** – CTIF provides timely feedback to the competent requested authorities on the use and usefulness of information obtained (see C.40.10).⁴ BNB and FSMA systematically provide feedback to requested authorities (either under bilateral co-operation agreements or pursuant to European law). The Federal Police states that it provides feedback on its TF investigations on request (without any specific legal obligation). AGDA provides feedback on the use and usefulness of information obtained (on request in the case of a spontaneous exchange) on the basis of cited legal instruments governing international mutual assistance, whether administrative or criminal (e.g. Regulation 515/97, Naples II Convention); feedback is also provided when the information provided discloses the commission of offences.

2 **CTIF:** Art. 22 al. 2 and 35 of the Law of 11 January 1993; **Federal Police:** multilateral treaties (Prüm Convention, application Convention for the Schengen Agreement, Interpol and Europol channels, etc.), bilateral treaties with non-Member States; **AGDA:** Reg. 515/97, Naples II Convention and the law on assent of 13 September 2004; other Customs mutual administrative assistance agreements and protocols with non-Member States; Council Directive 2011/16/EU on administrative co-operation in the field of taxation; multilateral Convention on mutual administrative assistance in tax matters as amended in 2010; double taxation treaties and agreements for the exchange of information on tax matters; **BNB** and **FSMA:** art. 36/16 of the Law of 22 February 1998; art. 77 of the Law of 2 August 2002.

3 **CTIF:** Egmont Secure Web, FIU-Net; **Federal Police:** Schengen information system.

4 **CTIF:** Art. 35 of the Law of 11 January 1993, Framework Decision 2000/642/JAI.

INTERNATIONAL COOPERATION

a8.36. **Criterion 40.5** – As for the four points of this criterion, the information provided by the competent authorities discloses no refusal of exchange or any unreasonable or unduly restrictive conditions to exchange of information.⁵

a8.37. **Criterion 40.6** – The competent authorities have established monitoring and protective measures to ensure that exchanged information is only used, save for prior authorisation, for and by the authorities for which the information was sought or provided.⁶

a8.38. **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.⁷

a8.39. **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.⁸ Requests for information to CTIF from foreign FIUs (financial intelligence units) are treated as STRs (suspicious transaction reports). It may therefore use all powers in the AML/CFT Law to process such reports.

a8.40. **Criterion 40.9** – CTIF has appropriate legal tools for co-operating with its foreign counterparts on ML, underlying predicate offences and TF (see C.40.1 and C.40.2). CTIF is also active in spontaneous information exchange.

a8.41. **Criterion 40.10** – If so requested, CTIF completes and returns a ‘feedback statement’ in respect of information provided by foreign FIUs. Moreover, 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.

a8.42. **Criterion 40.11** – The AML/CFT Law only enables CTIF to obtain co-operation from another FIU when there is a valid ‘referral by a declaration made by a person defined in the law (see R 20). If it receives a request for information from a foreign counterpart, CTIF may use all the powers granted to it by the AML/CFT Law to deal with suspicious declarations, and may collect any information it is able directly or indirectly to access and obtain.

a8.43. **Criterion 40.12** – BNB and FSMA have an appropriate legal basis for co-operation with their foreign counterparts.⁹ As for the other financial sector regulatory authorities, neither **FPS Economy** (responsible for

5 **CTIF** : Law of 11 January 1993; **Federal Police**: application convention for the Schengen Agreement, Art. 39 to 46; **AGDA**: Art. 19, Naples II Convention; **BNB**: Art. 36/14, Law of 22 February 1998; **FSMA**: Art. 77 §2, Law of 2 August 2002.

6 **CTIF**: Art. 17, Law of 11 January 1993; Art. 458 CP; **Federal Police**: Art. 44, Law of 5 August 1992; Art. 458 CP; **AGDA**: Art. 34 and S., Reg.515/97; **BNB**: Art. 36/17 §1er 3°, Law of 22 February 1998; **FSMA**: Art. 75 §2, Law of 2 August 2002.

7 **CTIF**: Art. 35, Law of 11 January 1993; Art.458 CP; **Federal Police**: Circulars COL2/2000 and MFO-3; art. 458 CP; **AGDA**: Art. 320 of the general Customs & Excise law; **BNB** and **FSMA**: Art. 36/17, §1er, 3°, and §4, Law of 22 February 1998; Art. 77bis, §1er, b), 3°, and §5, Law of 2 August 2002.

8 **CTIF**: Art. 22 al. 2, Law of 11 January 1993; **Federal Police**: Joint Directive MFO-3 of the Interior and Justice Ministries; **AGDA**: Reg.515/97 and Art. 8, Naples II Convention; **BNB**: Art. 36/17, Law of 22 February 1998; **FSMA**: Art. 77bis, Law of 2 August 2002.

9 **BNB**: Art. 36/16, Law of 22 February 1998; **FSMA**: Art. 77, Law of 2 August 2002. Certain sectoral laws also contain relevant provisions in this field (insurance agents, asset management companies and investment advisors,

monitoring consumer credit companies, financial leasing institutions and diamond traders; see R 26) nor **FPS Finance** (responsible for monitoring Bpost, which provides postal financial services; see R 26) provided information on the international co-operation they are authorised to implement.

a8.44. **Criterion 40.13** – BNB and FSMA are able to exchange domestically-accessible information with foreign counterparts. Pursuant to their respective laws and relevant European directives, they may depart from their obligation of professional secrecy and provide confidential information to competent foreign counterparts under a co-operation agreement. As stated in C.40.12, FPS Economy and FPS Finance are not able to exchange information internationally, as there is no legal basis for doing so.

a8.45. **Criterion 40.14** – Co-operation on supervising banking groups is organised at European level by the establishment of colleges of supervisors which facilitate the exchange of information and operational co-operation¹⁰ (see provisions cited in C.40.13).

a8.46. **Criterion 40.15** – The BNB refers to the provisions of article 36/16 of the Law of 22 February 1998, and states that the relevant measures are contained in laws governing transactions and supervision of banking groups.¹¹ More specifically, sectoral supervisory laws¹² set out the right of the competent authorities of an EEA Member State to seek information themselves in Belgium, after first advising the BNB or FSMA, unless the latter have undertaken such check for a foreign counterpart, in which case the foreign authority may be involved in its verification if it deems it necessary. For competent authorities in third-party States, the verification procedures are governed by the co-operation agreement between the BNB or FSMA and the authority concerned.

a8.47. **Criterion 40.16** – The BNB and FSMA must obtain prior authorisation from the requested supervisory authority for any disclosure or use of exchanged information. When BNB and FSMA receive confidential information, the information is covered by their legal obligations concerning professional secrecy. The information may only be used for the purpose of the enquiry for which it was provided. It may not be used for other purposes or transmitted to other persons or authorities without permission from the authority which provided it.¹³

a8.48. **Criterion 40.17** – The **Federal Police** services are able to exchange domestically-accessible information with their foreign counterparts for intelligence or investigation purposes in ML cases, underlying predicate offences and TF, including for identifying and tracing the proceeds and instruments of the crime (see C.40.2 and C.40.3). Council Decision 2007/845/JAI of 6 December 2007 concerning co-operation between

mutual fund companies).

10 [Directive 2009/111/EC of 16 September 2009](#); [Directive 2009/138/EC of 25 November 2009](#); [Law of 28 July 2011](#); Law of 25 April 2014 (Art. 158 to 162 and 319 to 326); [Law of 6 April 1995](#) (Art. 95, §5^{ter} and §5^{quater}); [RD of 12 August 1994](#) (Art. 9^{bis} to 13).

11 Law of 25 April 2014 Art. 158 to 162 (foreign branches of Belgian firms) and 319 to 326 (branches of foreign firms in Belgium); [Law of 6 April 1995](#) (Art. 95, §5^{ter} en §5^{quater}); [RD of 20 December 1995](#) (Art. 9); [Law of 9 July 1975](#) (Art. 70); [Law of 21 December 2009](#) (Art. 47).

12 Credit institutions: Art. 217, §2 and 324, Law of 25 April 2014; insurance companies: Art. 70 and 91^{septies}, §3 of the Law of 9 July 1975; stockbrokers: Art. 13, RD of 12 August 1994 and Art. 9, RD of 21 December 1995; re-insurers: Art. 87, §3 of the Law of 16 February 2009; payment institutions: Art. 42 of the Law of 21 December 2009; investment management companies and investment advisers: Art. 95, §§5, 5^{ter} and 5^{quater} of the Law of 6 April 1995 and Art. 9^{bis} to 13 of the RD of 12 August 1994; collective investment fund companies: Art. 241, §5 of the Law of 3 August 2012 and Art. 9^{bis} to 13 of the RD of 12 August 1994.

13 **BNB**: Art. 36/17, §3 and §4, Law of 22 February 1998; **FSMA**: Art. 77^{bis}, §4 and §5, Law of 2 August 2002.

INTERNATIONAL COOPERATION

asset recovery offices of the Member States in the field of tracing and identification of proceeds from or other property related to crime provides for prompt exchange of information enabling effective combatting of cross-border organised crime.

a8.49. **Criterion 40.18** – Police co-operation takes place particularly within the legal framework of conventions signed by Interpol, Europol or Eurojust with third-party countries.

a8.50. **Criterion 40.19** – Joint investigation teams (JITs) are established by the Law of 9 December 2004 on international mutual legal assistance in criminal matters, which incorporates into Belgian law the provisions of the Council Act of 29 May 2000 establishing the convention on mutual legal assistance in criminal matters between EU Member States, and Council Framework Decision 2002/465/JAI of 13 June 2002 on joint investigation teams. In Customs cases, the joint investigation team is one of the special forms of cross-border co-operation established by Part IV of the Naples II Convention.

a8.51. **Criterion 40.20** – As for exchanges of information between non-counterpart authorities, indirect exchange with CTIF is not expressly provided in the AML/CFT Law. The authorities state that such exchanges are nonetheless possible. There is no formal mechanism enabling the Federal Police to make such exchanges. No mechanism exists for exchange of information between foreign non-counterpart authorities and customs.

Weighting and conclusion

a8.52. Exchange of information between non-counterpart authorities is not clearly provided for in Belgium. Moreover, two of the supervisory authorities (FPS Economy and FPS Finance) lack the capacity to co-operate with foreign authorities having comparable powers. **Belgium is largely compliant with R 40.**



A8

ACRONYMS

AGDA	<i>Administration générale des douanes et accises</i> (Belgian Customs & Excise)
AISBL	<i>Association internationale sans but lucratif</i> (international non-profit association)
AML/CFT	Anti-money laundering / counter-terrorist financing
Art.	Article / Articles
ASBL	<i>Association sans but lucratif</i> (non-profit association)
BCE	<i>Banque Carrefour Entreprises</i> (Belgian Companies Register)
BNB	<i>Banque Nationale de Belgique</i> (National Bank of Belgium)
BNI	Bearer negotiable instruments
C.	Criterion
CAF	Service de coordination anti-fraude de l'inspection spéciale des impôts
CBFA	<i>Commission bancaire, financière et des assurances</i> (former Belgian financial supervisor)
CCLBC	<i>Collège de coordination de la lutte contre le blanchiment de capitaux d'origine illicite</i> (College for AML Co-ordination)
CIC	<i>Code d'instruction criminelle</i> (Criminal Instruction Code)
CPC	<i>Code de procédure criminelle</i> (Criminal Procedure Code)
CRS	<i>Collège du renseignement et de la sécurité</i> (College for Intelligence and Security)
CTIF	<i>Cellule de traitement des informations financières</i> (Belgian FIU)
DJF	Direction de la lutte contre la criminalité économique et financière de la police
DJP	Direction de la lutte contre la criminalité contre les personnes
DNFBP	Designated non-financial businesses and professions
ECB	European Central Bank
EU	European Union
FATF	Financial Action Task Force
FIU	Financial intelligence unit
FSMA	Financial Services and Markets Authority (<i>Autorité des services et des marchés financiers</i>)
GDP	Gross domestic product
IEC	<i>Institut des Experts comptables et des Conseils fiscaux</i> (Institute of Chartered Accountants and Tax Consultants)
IN	Interpretative Note
IO	Immediate outcome
IPCF	<i>Institut Professionnel des Comptables et Fiscalistes Agréés</i> (Professional Institute of Certified Accountants and Tax Accountants)
IRE	<i>Institut des Réviseurs d'Entreprises</i> (Institute of Statutory Auditors)
ISI	Inspection Spéciale des Impôts
JIT	Joint investigation team
MD	Ministerial decree (Arrêté ministériel)

ACRONYMS

MER	Mutual evaluation report
ML	Money laundering
MoU	Memorandum of understanding
MVTS	Money or value transfer service
NPO	Non-profit organisation
OCAM	<i>Organe centrale pour l'analyse de la menace</i> (Central Unit for Threat Analysis)
OCDEFO	<i>Office Central de la lutte contre la Délinquance Économique et Financière Organisée</i> (Central Unit for Combatting Economic and Organised Financial Crime)
OCSC	<i>Organe central pour la saisie et la confiscation</i> (Central Unit for Seizure and Confiscation)
OECD	Organisation for Economic Co-operation and Development
OLAF	<i>Office européen de lutte anti-fraude</i> (European Anti-Fraud Office)
Para.	Paragraph
PC	<i>Code pénal</i> (Penal Code)
PEP	Politically exposed person
PF	Financing of the proliferation of weapons of mass destruction
PJF	Directions judiciaires déconcentrées
Plan R	Plan radicalisme
R	FATF Recommendation
RD	Royal Decree (<i>Arrêté royal</i>)
Reg.	Regulation
SA	<i>Société anonyme</i> (public limited company)
SCA	<i>Société en commandite par actions</i> (company with liability limited by shares)
SCRI	<i>Société coopérative à responsabilité illimitée</i> (unlimited-liability co-operative company)
SCRL	<i>Société coopérative à responsabilité limitée</i> (limited-liability co-operative company)
SE	<i>Sûreté de l'État</i> (State Security Service)
SGRS	<i>Service Général du Renseignement et de la Sécurité</i> (General [military] Intelligence and Security Service)
SNC	<i>Société en nom collectif</i> (general partnership)
SPF	<i>Service public fédéral</i> (Federal Public Service = Belgian Federal Ministry)
SPRL	<i>Société privée à responsabilité limitée</i> (private limited-liability company)
SR	FATF Special Recommendation (before the 2012 revision)
STR	Suspicious transaction report
TC	Technical compliance
TF	Terrorist financing
TFS	Targeted financial sanctions
UNSCR	United Nations Security Council Resolution

The FATF logo is a red shield-shaped emblem with the acronym 'FATF' in white, bold, sans-serif capital letters at the top. Below the text are three stylized, overlapping white shapes that resemble leaves or petals, arranged in a fan-like pattern. The entire logo is set against a dark red background.

FATF

© FATF

www.fatf-gafi.org

April 2015

Anti-money laundering and counter-terrorist financing measures - Belgium *Fourth Round Mutual Evaluation Report*

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CFT) measures in place in Belgium as at the date of the on-site visit (30 June to 15 July 2014). The report analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Belgium's AML/CFT system, and provides recommendations on how the system could be strengthened.