Commission de Surveillance
du Secteur Financier

Annual report 2025

XXII. Financial crime

This chapter focuses on key aspects or major events of the CSSF's 2025 AML/CFT supervisory missions and supervision of the implementation of the restrictive measures in financial matters in relation to the different categories of professionals supervised, authorised or registered by it as regards their compliance with the relevant professional obligations. Section 2 provides information on the main developments in the legal and regulatory framework, as well as feedback on AML/CFT-related work carried out at national, European and international level.

- **New "Fight against Financial crime" department**

In 2025, a department entirely dedicated to the fight against financial crime ("Fight against Financial crime" department or "LCF department") was set up as a result of the reorganisation of the former department "Consumer Protection/ Financial Crime" which was composed of several divisions. The new LCF department counts 12 staff members and two divisions, whose main missions are (i) dealing with legal matters pertaining to the fight against financial crime as a whole, which includes money laundering, terrorist financing and proliferation financing (AML/TF/PF) or predicate money laundering offences, such as corruption, or also restrictive measures in financial matters, and (ii) steering, coordinating and supporting the CSSF's actions relating to the fight against financial crime at an internal, national, European and international level.

The LCF department plays a strategic role at national level through its active contribution to the drafting and evolution of the legal and regulatory framework, and its close cooperation with the other national competent authorities and self-regulatory bodies.

At international level, the LCF department participates in the development of European standards and cooperates with the European or international competent authorities, in particular with the new European Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). An example for this cooperation is the LCF department representing the CSSF in the Financial Action Task Force's (FATF) work and meetings, and coordinating and implementing the CSSF's actions to ensure its compliance with the FATF standards.

1. AML/CFT supervision and supervision of restrictive measures in financial matters by the CSSF

Controlling compliance with professional obligations in relation to AML/CFT and restrictive measures in financial matters is an integral part of the supervisory framework put in place by the CSSF. This control programme combines off-site and on-site supervisory measures and follows a risk-based approach, which relies on different sets of information and data gathered by the CSSF during the year on the risks and mitigation measures implemented by the professionals. To this end, the AML/CFT supervisory departments transmit an AML/CFT questionnaire to the professionals under their supervision, whose outcome will contribute to the annual risk assessment of each entity by adapting the intensity of supervision.

1.1. Off-site AML/CFT supervision

1.1.1. Credit institutions and central securities depositories (CSDs)

In 2025, the CSSF continued its off-site AML/CFT supervisory actions to ensure that credit institutions and CSDs maintain effective arrangements in relation to the fight against terrorist financing and restrictive measures in financial matters.

In this evolving EU regulatory context, the CSSF intensified its exchanges with the Luxembourg banking sector, in particular through meetings and regular contacts with the credit institutions' compliance officers and members of the management body (in its supervisory and management function). Thus, 192 meetings relating specifically to AML/CFT aspects were organised in 2025. It is worth mentioning that these exchanges were complemented by an AML/CFT conference for credit institutions organised jointly with the ABBL, with the participation of the Financial Intelligence Unit (FIU), which was held on 24 April 2025. A total of five meetings of the Expert Working Group Compliance, established with the ABBL and the FIU, were held in order to discuss in particular the development of risks linked to virtual IBANs and corruption, the implementation of the European regulation on instant credit transfers and the regulatory technical standards (RTS) that AMLA submitted to public consultation.

In parallel, the CSSF organised five AML/CFT college meetings in its role as lead supervisor out of a total of 17 colleges and participated in 24 AML/CFT college meetings organised by European authorities for 32 Luxembourg credit institutions.

The CSSF identified deficiencies resulting from the fact that certain high-risk countries had not been taken into consideration as well as recurring delays in the periodic review process. The CSSF sent seven injunction letters in this context.

1.1.2. Investment firms

The investment firm sector is a relatively heterogeneous sector, encompassing a number of supervised entities that provide quite diverse investment services and activities, whilst remaining subject to the same AML/CFT professional obligations.

In 2025, the attention points focused on raising the sector's awareness of the future developments linked to the EU AML/CFT regulatory package, published in June 2024, which established in particular the AMLA. The focus was also on following up on the recommendations identified by the FATF in its fourth mutual evaluation report of Luxembourg, especially as regards enhancing the TF risk understanding and improving the quality of the reports sent to the FIU.

In this context, the dedicated AML/CFT team within the "Supervision of investment firms" department recruited a new team member, bringing its total headcount to four as at 31 December 2025.

During the year, the CSSF conducted a targeted review addressing the issue of RR[1] and RC[2] mandates being held concurrently within investment firms. Moreover, a thematic review on AML/CFT risks linked to trust and company service providers (TCSP) was carried out. At a conference held in March 2025, organised in collaboration with the FIU, the supervisory priorities and attention points retained for 2025 were presented to the sector, and good practices linked to the applicable AML/CFT obligations were shared, in particular in relation to the annual compliance/AML-CFT report,

1 Person responsible for compliance with the professional obligations as defined in CSSF Regulation No 12-02

2 Compliance officer in charge of the control of compliance with the professional obligations as defined in CSSF Regulation No 12-02

transaction monitoring, the risk-based approach and the risk assessment.

In 2025, as far as European cooperation is concerned, the CSSF organised two AML/CFT college meetings involving two investment firms in its role as lead supervisor, and it actively used the information exchange channels set up with other authorities in relation to other four investment firms.

As for all CSSF AML/CFT teams, the dedicated AML/CFT team of the department also actively contributed to the review of level 2 and level 3 EU texts putting into practice the new rules introduced by the EU AML/CFT regulatory package. The AML/CFT team also contributed to the update of the appendix concerning investment firms in the *Sub-sector Risk Assessment on TCSP* (TCSP SSRA) as published in January 2026.

As part of its off-site controls, the CSSF met with the chief compliance officers of eight investment firms in 2025. Moreover, it intensified direct and informal contacts (via email and phone) with the supervised entities and participated in two welcome visits at the premises of newly authorised investment firms. The off-site controls resulted in ten observation letters that referred to weaknesses in the update of AML/CFT policies and procedures, transaction monitoring and the follow-up, within the AML/CFT report drawn up by the RC, to the recommendations drawn up by the third line of defence. In addition, two injunction letters relating to weaknesses identified in the periodic customer review system were sent out.

The dedicated AML/CFT team also followed up on the weaknesses identified during the on-site inspections carried out by the on-site inspection team at investment firms and on the relevant remediation plans.

1.1.3. Specialised PFS

Specialised professionals of the financial sector ("specialised PFS") hold different authorisations, e.g. as corporate domiciliation agent, professional providing company incorporation and management services, registrar agent, professional depositary of financial instruments, professional depositary of assets other than financial instruments, operator of a regulated market authorised in Luxembourg, debt recovery, professional performing lending operations, professional performing securities lending, Family Office and mutual savings fund administrator.

The CSSF established a series of off-site supervisory measures to verify the specialised PFS' compliance with their AML/CFT obligations through a risk-based approach. Specialised PFS providing company services (TCSP activities) pose a high inherent ML/TF risk. To comply with their legal AML/CFT obligations, they must implement mitigation measures to reduce their risk exposure.

The human resources dedicated to the off-site AML/CFT team of the "Supervision of specialised PFS" department, set up as a division since 1 December 2025, remained stable with five agents.

The annual AML/CFT conference dedicated to specialised PFS, whose purpose is to provide information and training to supervised entities, was organised on 27 January 2025 with the participation of the FIU. A total of 352 participants attended the conference. It should be noted that mortgage credit intermediaries had also been invited.

As regards cooperation with the private sector in 2025, the CSSF held three meetings with the working group dedicated to specialised PFS in collaboration with the FIU, the Luxembourg Association of Compliance Officers (ALCO), the Luxembourg Alternative Administrators Association (L3A), the Luxembourg Private Equity and Venture Capital Association (LPEA), the Luxembourg Association of Family Offices (LAFO) and the Luxembourg Association for Risk Management (ALRiM). The meetings concerned, i.a. (i) the update of the *Sub-Sector Risk Assessment on TCSP* for specialised PFS, (ii) the public consultation on the regulatory technical standards based on Article 28(1) of Regulation (EU) 2024/1624, (iii) the outcome of the thematic off-site inspection on the use of shelf companies by specialised PFS providing TCSP services, and (iv) the 2025 thematic missions on the definition of ML/TF risk appetite and terrorist financing.

In 2025, 15 meetings with specialised PFS covered specific AML/CFT topics, such as the activities of specialised PFS and the ML/TF risk to which they are exposed, the systems and the use of new technologies, training and resources put in place with respect to AML/CFT and compliance, the supervision of AML/CFT delegated tasks, where applicable, the involvement of members of the board of directors and/or of the board of managers in projects relating to AML/CFT, AML/CFT and compliance projects, where applicable, the cooperation with the authorities, etc. The fight against terrorist financing, the politically exposed persons (i.e. their detection, case management and the exposure of specialised PFS to corruption risk) and the sanctions issued notably against entities and individuals in the context of the Ukraine conflict and the financing of the proliferation of weapons of mass destruction were also on the agenda of the meetings.

In 2025, AML/CFT controls were carried out during three welcome visits. These controls included, among other things, tests on the customer name screening tool, the review of AML/CFT files and the presentation by the specialised PFS of its ML/TF risk, its risk appetite, its AML/CFT procedures and its transaction monitoring process.

A total of 14 observation letters were sent to specialised PFS with respect to shortcomings identified notably (i) in the reports issued as part of the closing documents for the year 2024, (ii) in the 2024 annual AML Questionnaire on Financial Crime, (iii) following face-to-face meetings at the premises of the CSSF, (iv) during control welcome visits of the CSSF at newly authorised specialised PFS, (v) during the follow-up process of on-site inspections and (vi) following the review of the AML/CFT procedures during the licencing process.

After reviewing the appointments proposed by the specialised PFS for the roles of RC, compliance officer and RR, a total of 14 acknowledgement letters were sent.

1.1.4. Payment institutions and electronic money institutions

The CSSF is in charge of the AML/CFT supervision of payment institutions and electronic money institutions established in Luxembourg and authorised by the CSSF, as well as of branches, agents and distributors established in Luxembourg of payment institutions or electronic money institutions authorised in other EU Member States.

As part of its off-site ML/TF risk supervision of these players, the CSSF carried out a number of actions in 2025, including ML/TF risk awareness-raising actions in relation to this specific sector, such as:

- the organisation of an annual conference on specific themes pertaining to payment institutions and electronic money institutions, branches and agents or distributors of foreign institutions established in Luxembourg, as well as virtual asset service providers/crypto-asset service providers. Among the topics presented during this conference for the payment sector players, the CSSF provided information on the evolution of ML/TF risks to which these entities are or may be exposed, on the trends observed and the expected emerging risks in Luxembourg, as well as information on the deficiencies that are recurrently noted by the CSSF as part of its AML/CFT supervision of these players;

- the launch of a thematic review relating to the CFT framework including on-site visits at the premises of eight payment and electronic money institutions;

- the continuation of national and international cooperation work, including notably regular exchanges and discussions between the CSSF and the FIU, the organisation of and participation in the AML/CFT colleges as well as the organisation of bilateral meetings with other national authorities depending on the AML/CFT supervisory needs of these players.

Moreover, the exchanges with the institutions in the context of this AML/CFT supervision notably covered the following topics:

- the requirements relating to adequate internal management, in particular adequate and sufficient human resources to mitigate and effectively manage the ML/TF risks to which institutions are or will be exposed when developing, where applicable, new products, services or markets;

- the adequacy, assessment and update of the parameters, criteria or scenarios defined by the institutions while exercising ongoing due diligence on the transactions concluded by their customers, including the parameters, criteria and scenarios linked to terrorist financing, tax crimes, complex and unusual transactions;

- the implementation of a control plan by the compliance function (second line of defence) to verify the quality and compliance of the controls carried out by the internal and, where applicable, outsourced teams of the first line of defence, and to contribute to the independent control of ML/TF risks.

1.1.5. Virtual asset service providers/ Crypto-asset service providers

The CSSF is in charge of the AML/CFT supervision of virtual asset service providers (VASPs) registered by the CSSF in accordance with Article 7-1 of the Law of 12 November 2004 on AML/CFT as in force on 30 December 2024, and of crypto-asset service providers (CASPs) authorised in accordance with the new framework provided for under MiCAR.

As part of its off-site ML/TF risk supervision of these players in 2025, the CSSF carried out a number of actions, including ML/TF risk awareness-raising actions in relation to this specific sector, such as:

- the preparation of an internal sectoral analysis of the risks applicable to VASPs/CASPs, taking into account the sector's major developments and the ML/TF risks to which this sector is exposed;

- the organisation of an annual conference on specific themes pertaining to payment institutions and electronic money institutions, branches and agents or distributors of foreign institutions established in Luxembourg, as well as to VASPs/CASPs. Among the topics presented during this conference for the crypto-assets sector players, the CSSF provided information on the evolution of ML/TF risks to which these entities are exposed, on the trends observed and the expected emerging risks in Luxembourg, as well as information on the regulatory requirements linked to Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, and more specifically on the Travel Rule, as well as in relation to its practical implementation for Luxembourg players;

- the launch of a thematic review relating to the CFT framework including on-site visits at the premises of two CASPs. This review is carried out jointly with the similar review carried out in the payments sector (cf. Section 1.1.4. above);

- the continuation of national and international cooperation work, including notably regular exchanges and discussions between the CSSF and the FIU, and a number of bilateral exchanges with other national authorities depending on the AML/CFT supervisory needs of these players.

Moreover, as for the payments sector players, the exchanges with the institutions in the context of this AML/CFT supervision notably covered the following topics:

- the requirements relating to adequate internal management, in particular adequate and sufficient human and technical resources to mitigate and effectively manage the ML/TF risks to which institutions are exposed. Considering the emergence and growth of the crypto-asset sector in Europe, hiring and retaining staff with proper understanding of the specificities of crypto-assets, the related services and their AML/CFT risks requires appropriate investments in terms of both recruitment and training at the level of VASPs/CASPs;

- the adequacy of the parameters, criteria or scenarios defined by the institutions as well as the use of blockchain analysis tools while conducting ongoing due diligence on the transactions concluded by their customers;

- the implementation of a control plan by the compliance function (second line of defence) to verify the quality and compliance of the controls carried out by the internal and, where applicable, outsourced teams of the first line of defence, and to contribute to the independent control of ML/TF risk.

1.1.6. Investment fund managers and UCIs

This sector consists of products (investment funds) and their managers (management companies). No significant developments occurred in this sector in 2025.

The CSSF implemented the off-site supervision plan in accordance with the CSSF's objectives, focusing on a risk-based approach. A particular emphasis was placed on the fight against terrorist financing.

An updated version of the UCI sub-sector risk assessment was published. This new version illustrates that the professionals in Luxembourg continuously adapt their control arrangements to the ever-changing ML threats, while confirming the low level of residual TF risk. Moreover, in December 2025, the CSSF organised the annual "UCI department" conference in cooperation with the FIU and the Administration de l'Enregistrement, des Domaines et de la TVA, attended by more than 1,400 participants.

In addition to the fight against terrorist financing, the CSSF led specific projects on risk appetite, on the risk-based approach and on training programmes.

The CSSF carried out 6,135 off-site supervisory measures, including 57 bilateral meetings and 34 AML/CFT supervisory colleges. The increase in off-site supervisory measures notably results from the automated report analysis and from large-scale automated thematic reviews concerning name screening and the risk-based approach. In total, 504 observation letters were sent; this figure is notably linked to the increased number of automated measures.

The CSSF imposed 9 administrative sanctions for non-filing of the AML/CFT reports.

1.2. On-site AML/CFT supervision

AML/CFT on-site inspections are carried out by the "On-Site Inspection" (OSI) department at all the professionals supervised by the CSSF in order to assess that the quality of the AML/CFT framework is in line with the legal and regulatory requirements. Only management companies (when exercising a collective management activity for investment funds) are subject to separate on-site supervision (via the "UCI on-site inspection" department, whose controls on the delegation of AML/CFT tasks are described below).

Every year, the teams in charge of off-site supervision identify the professionals that will be subject to an on-site inspection. In addition to the global inherent risk relating to the sector of activity, the frequency of the controls depends on the AML/CFT risk measured for each professional (taking into account its activity, its customer base, the deficiencies identified by the compliance function and/or by the internal and external auditors, etc.). On-site inspections are then carried out independently by the agents specialised in AML/CFT of the OSI department.

In 2025, the OSI department carried out 37 AML/CFT inspections, covering a large range of professionals supervised by the CSSF, including banks, specialised PFS, investment firms, management companies (performing the activity of transfer agent or individual discretionary portfolio management), electronic money institutions, payment institutions or crypto-asset service providers. Although the outcome of these inspections was globally positive as regards the quality of the AML/CFT arrangements put in place, the CSSF imposed four sanctions in 2025 following the on-site inspections carried out during the previous years.

In the continuity of the FATF visit, the OSI department intended to focus on the measures taken by professionals to specifically tackle the fight against terrorist financing during its on-site inspections carried out in 2025. However, instead of initiating thematic on-site inspections limited to this specific topic, the OSI department decided to consider terrorist financing as an attention point that had to be taken into account systematically for each AML/CFT on-site inspection in 2025. This allowed for broader coverage and a better understanding of how this topic is addressed by the supervised professionals.

In this context, certain good practices can be highlighted, such as the performance of an assessment dedicated to terrorist financing within the annual risk assessment of the professional's activities, taking into account specific terrorist financing risk factors when assessing country risk (e.g. by considering the Global Terrorism Index) and when assessing client risk (e.g. via the activity), the implementation of transactional analysis scenarios enabling notably the identification of TF cash flows, the identification of certain key words in the payment messages or the incorporation of a TF module into the training sessions for its staff.

A similar approach will be applied in the future for other topics which the OECD, the FATF or the national AML/CFT strategy singles out, as for example the risk related to the laundering of the proceeds of (active and passive) corruption, the risk of financing the proliferation of weapons of mass destruction or also compliance with restrictive measures/international financial sanctions.

Through the on-site inspections, the agents of the OSI department acquire a transversal view of the market practices and they can use this experience beyond on-site inspections. For instance, they can share AML/CFT best practices in the context of public-private partnerships (e.g. ABBL conferences, etc.) or participate in AMLA working groups defining the future European AML/CFT standards.

Several specific issues were identified during the on-site inspections performed in 2025, which should be brought to the attention of all the professionals supervised by the CSSF.

Professionals should pay particular attention to the quality of their customer database, notably when data is pre-filled by the customers themselves. Indeed, even the best risk scoring tools (i.e. tools for the assessment of AML/CFT risk of customers) or name screening tools (i.e. tools for the identification of persons, entities or groups subject to restrictive measures in financial matters, politically exposed persons, as well as persons subject to negative information or referred to in enquiries by competent authorities) are not fully effective if they are connected to databases containing incomplete or erroneous data.

To ensure that professionals are able to apply restrictive measures in financial matters without delay, where necessary, the CSSF reiterates that the alerts of the name screening tools (i.e. the screening of the customer and transaction counterparties database) must be dealt with without delay where these alerts concern persons, entities or groups subject to restrictive measures in financial matters. Moreover, if the professional is not in a position to swiftly deal with the alert, the professional must take all measures to ensure that potential restrictive measures can be applied.

For professionals offering financial services to businesses, mainly in the context of e-commerce, a good practice consists in identifying any divergence between the nature of the businesses' activity and the products offered, and verifying the existence of price gaps that are manifestly abnormal between brand products sold on the market and those sold by those businesses.

The on-site inspections revealed that certain professionals adopted innovative AML/CFT tools and methods. These tools mostly aim to strengthen client data verification (e.g. detection of forged documents, facial video comparison with ID documents, etc.), to enhance ML/TF risk measure (exploiting for example the clients' location data, such as IP addresses or geolocation data from smartphones used for the connection, etc.) or to improve transaction analysis scenarios (for example by defining dynamically "normal" transaction types for a cluster of clients sharing the same characteristics and, in a second step, identifying the atypical transactions for this cluster). Professionals should remain responsive to these new market practices and should not hesitate to question their historical AML/CFT controls in order to improve them. However, these innovative tools are sometimes relatively complex (notably when AI-based) and professionals should always maintain control of these tools, understand them and be in a position to demonstrate their proper functioning (via regular and formalised controls).

The OSI department agents observed that professionals usually transmit the required reports to the FIU when they suspect ML/TF concerning a customer. However, professionals must perform an enhanced monitoring of the customer concerned to prevent any further suspicious transactions, and, where applicable, send a complementary suspicious transaction report to the FIU.

The second level controls are sometimes located outside Luxembourg, within a central team in charge of the supervision of a number of subsidiaries or branches belonging to a same group. In that case, the Luxembourg professional should keep access to the work specifically carried out for Luxembourg and the outcome thereof.

Finally, the CSSF understands that professionals attempt to rationalise their AML/CFT controls and to optimise the related costs by defining very codified check lists on their KYC documents to be collected depending on the type of client concerned. However, as already mentioned at certain conferences, the CSSF reiterates that an AML/CFT analysis should not be limited to a mere collection of documents and their update during periodic reviews. A more appropriate analytical approach would be to take a step back to verify (notably during the periodic reviews) whether the functioning of the account (and the transactions carried out) remains coherent with the customer's profile and the object and nature of the business relationship (as defined at the moment of the entry into business relationship).

For the collective management sector, the "UCI on-site inspection" department carried out, in 2025, nineteen inspections at investment fund managers and alternative investment fund managers.

- **Key areas for improvement**

The missions completed during the year gave rise to the following major observations at certain entities:

- Weaknesses regarding the obligation to detect persons, entities and groups subject to prohibitions or restrictive financial measures, as provided for in Article 3(2)(d) of the Law of 12 November 2004 on AML/CFT and Article 39(2) of CSSF Regulation No 12-02 (namely an important backlog of a high number of open alerts untreated for several months, insufficient formalisation of treatment as false positive alerts as well as incomplete controls for distributors and discretionary portfolio management customers, which had not been added to the database).

- Weakness with respect to cooperation with AML/CFT authorities in cases of delayed filing of suspicious activity reports (STRs/SARs) several months after the refusal of a transaction in contravention to Article 5(1)(a) of the Law of 12 November 2004 on AML/CFT according to which "professionals, their directors (*dirigeants*, members of the authorised management) and employees are required to inform promptly, on their own initiative, the FIU when they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing is being committed or has been committed or attempted, in particular in consideration of the person concerned, its development, the origin of the funds, the purpose, nature and procedure of the operation."

- Weaknesses with respect to the scope and outcome of the Compliance Officer's regular controls and verifications, as set forth by Article 42(5) of CSSF Regulation No 12-02 as well as a lack of follow-up to ensure that previous observations were adequately addressed and remediated by the entity concerned in accordance with Article 44 of CSSF Regulation No 12-02.

- **Thematic inspection on blocked accounts**

In the context of the observations made by the FATF regarding the significant number of blocked accounts held with financial institutions in Luxembourg, the "UCI on-site inspection" department included this topic in its on-site inspection programme for 2025 and selected five IFMs based on the information on blocked accounts at its disposal.

The inspections carried out showed that only a limited proportion of blocked accounts relate to situations presenting a concrete AML/CFT risk. The analysis showed that most blockings resulted from periodic reviews and updates of documents, data and information in accordance with Article 35 of CSSF Regulation No 12-02 (often referred to as KYC refresh exercises). In this respect, it was observed that many blockings occur in situations involving the re-collection of expired identification documents, such as passports or equivalent documents obtained for identification and verification purposes.

- **Good practices detected during thematic inspections**

During the course of the inspections the CSSF identified the following good practices:

- the implementation of a framework distinguishing accounts blocked for AML/CFT-related reasons from those blocked for periodic review purposes, thereby enabling a more accurate assessment of the actual AML/CFT risk;
- the inclusion of specific tests relating to blocked accounts as part of the periodic reviews of delegates responsible for maintaining the investor register;
- regular reporting to the boards of directors of the funds on the status of blocked accounts, as well as on blocking and unblocking measures taken.

The verifications performed as part of the thematic inspections did not reveal any major weaknesses.

- **Guidance for AML/CFT blocking**

IFMs are encouraged to assess during their periodic customer information review or upon trigger events, the update of an expired identity document (or equivalent) obtained for identification and verification purposes in view of (i) the risk associated with the customer, (ii) the type of identity document as well as (iii) any potential doubts regarding the continued accuracy of the identification data held.

The CSSF does not require blocking solely for the reason that an identification document (or equivalent) has expired or that a periodic review is or will be done. However, an account should be blocked in this context for AML/CFT reasons in particular when specific risks are identified or in case of doubts as to the accuracy of the customer's identification details.

- **CSSF Conference**

During the annual AML/CFT conference for the collective management sector on 4 December 2025, the CSSF shared examples of findings (in particular high and medium-high risk findings) identified during recent on-site AML/CFT inspections.

The presentation also offered insight on past thematic on-site inspections, mostly the thematic review on counter-proliferation financing controls and on best practices (cf. also CSSF publication dated 17 November 2025).

2. Development of the legal and regulatory framework

This section highlights the main legal and regulatory developments relating to the fight against financial crime at national, European and international level. It supplements the information published throughout the year on the CSSF's website or provided, inter alia, during the annual conferences and as part of the public-private partnerships (PPP) that the CSSF established with certain sectors (mentioned above).

2.1. Launch of activities of the new European AML/CFT authority

AMLA, the new European authority, formally established in 2024 and based in Frankfurt, started its activities in 2025. Several meetings of its most important governing body, the AMLA General Board, in which the CSSF took part as national member representing AML/CFT supervision in Luxembourg jointly with the Luxembourg FIU, representing the FIUs aspect, were held in 2025. AMLA's main missions may be summarised as follows:

- contributing to the identification and assessment of ML/TF risks;
- establishing the technical foundations providing details for the common regulatory framework;
- coordinating the supervision carried out by national supervisory authorities and ensuring consistent application of the rules in all Member States;
- supporting and coordinating FIUs to enhance information sharing.

In parallel with AMLA's start of operations including important staff recruitment, the establishment of its governance and the ramp-up of its IT systems, AMLA also defined its immediate and strategic objectives.

On the operational side, AMLA notably defined the following priorities:

- develop technical standards and guidance entailing specifications to the common regulatory framework;
- establish a common methodology for the risk assessment of obliged entities and select the more complex and higher risk entities for the purpose of direct supervision by AMLA starting mid-2028 and allow convergence of supervisory practices;
- promote a cooperation culture with respect to AML/CFT.

As far as strategic objectives are concerned, AMLA already announced that it would concentrate on the supervision of crypto-asset service providers.

It should also be noted that the EBA transferred its AML/CFT powers and mandates to AMLA as of 1 January 2026.

2.2. Strengthening the regulatory EU framework with respect to AML/CFT

AMLA was granted extended powers to develop about 40 projects relating to implementing/regulatory technical standards and guidance based on its establishing regulation (Regulation (EU) 2024/1620) and Regulation (EU) 2024/1624 defining notably professional obligations. The CSSF is fully committed, in coordination with the other national competent authorities and bodies, to the development of these technical standards and guidelines which will provide the financial sector, and also the non-financial sector, with important details on the new requirements as well as on the practices or formats to be used for the implementation of the AML package.

In this context, the financial sector was also asked to contribute to the public consultations on these draft technical standards on several occasions in 2025. The CSSF would like to thank all the players for their valuable contribution to the practical implementation of the EU texts.

2.3. High-risk countries and non-cooperative countries - EU lists

In June 2025, the EU Commission amended Commission Delegated Regulation (EU) 2016/1675 identifying high-risk third countries with strategic deficiencies (in their AML/CFT regimes), by adapting the list of these countries. Moreover, in August 2025, the EU Commission set a new identification criterion targeting from now on also high-risk third countries that are not subject to a call for action or under increased monitoring by the FATF, but whose FATF membership has been suspended. In this respect, the Russian Federation was added to the EU list in January 2026.

Moreover, as every year in February and October, the EU Council revised the list of non-cooperative jurisdictions for tax purposes.

2.4. Developments of the international AML/CFT framework: main FATF initiatives and actions

As every year, the CSSF participated in the FATF plenary sessions which took place in February, June and October 2025, with a specific focus on financial inclusion, asset recovery and AML/CFT risk supervision.

2.4.1. Developments related to the FATF's recommendations

The FATF focused on several strategic initiatives in 2025[3]. Among them, the financial inclusion initiative led to the revision of FATF Recommendation 1 ("Assessing risks & applying a risk-based approach") and its interpretive note. In parallel, the FATF developed new guidelines on the implementation of the risk-based approach, specifying that the latter aims at implementing enhanced supervision whenever necessary, but also at applying simplified measures whenever possible. These new guidelines include, in particular, measures aiming at addressing the de-risking phenomenon.

The purpose of a further strategic initiative that was finalised in 2025 was to increase payment transparency. In this context, FATF Recommendation 16 (Travel Rule) was amended. The key changes notably include an increased transparency of the information accompanying cross-border payments and the requirement to introduce protection tools against error and fraud.

In view of the situation in Iran[4], the FATF confirmed the re-application of UN resolutions against Iran within the scope of Recommendation 7 (Targeted financial sanctions relating to proliferation) in October 2025.

2.4.2. Other FATF publications of interest for the financial sector

The report on detecting and combating online child sexual exploitation provides a precise analysis of the financial flows behind live-streamed sexual abuse of children and financial sexual extortion of children (cf. CSSF Newsletter No 300 dated January 2026).

The report *Comprehensive Update on Terrorist Financing Risks* highlights the evolving nature of these risks and trends, as well as the terrorists' constantly adaptative capacity (cf. CSSF Newsletter No 302 dated March 2026).

The report concerning the reminder and the means of the global fight against proliferation financing describes how proliferation networks acquire dual-use goods and technologies, and knowledge thereof (cf. point 2.7. below and CSSF Newsletter No 295 dated August 2025).

During the year, the FATF underlined that strengthening cooperation and collaboration among all players is crucial. The importance of public-private partnerships (PPP) was reiterated at the Private Sector Collaborative Forum which was held in Mumbai in March 2025. The private sector is "at the forefront of the fight against financial crimes". As a response to globalisation of financial systems, the FATF, the Egmont Group, Interpol and the UN called for a stronger international cooperation and published a practical guide on international cooperation against money laundering.

3 Cf. CSSF Newsletter No 295 dated August 2025.

4 Cf. also point 2.6. below.

Finally, the first FATF mutual evaluations under the new methodology set out for the 5th round of evaluations were adopted in 2025 for the following FATF members: Belgium and Malaysia.

According to the provisional FATF calendar, Luxembourg will be evaluated in 2029-2031, with an on-site visit planned in June 2030.

2.4.3. Evolution of the FATF lists

During the 2025 FATF plenary meetings, Bolivia, Lao PDR, Nepal and the Virgin Islands (UK) were added to the FATF list of jurisdictions under increased monitoring - commonly referred to as the "grey list". Moreover, South Africa, Burkina Faso, Croatia, Mali, Mozambique, Nigeria, the Philippines and the United Republic of Tanzania were removed from this list.

The FATF high-risk jurisdictions list subject to a call for action, commonly referred to as the "blacklist", did not change. The FATF thus requires the application of enhanced due diligence, and, where necessary, countermeasures to protect the international financial system from the persistent risks emanating from the following three jurisdictions: Democratic People's Republic of Korea, Iran and Myanmar. The annex of Circular CSSF 22/822 is regularly updated and provides a complete overview.

2.5. International Organization of Securities Commissions (IOSCO)

The CSSF is strongly involved with IOSCO's AML/CFT activities, particularly with IOSCO's AML Network, currently chaired by the CSSF. For 2025, the webinar on emerging money laundering, terrorist financing and proliferation financing risks linked to crypto-assets and virtual assets is worth mentioning. The information shared concerned more specifically key statistical data, examples of red flag indicators and typologies.

2.6. Evolution of the national AML/CFT framework

2.6.1. Key amendment of the Penal Code

The Law of 12 December 2025 introduced a major modification to Article 506-1 of the Penal Code, replacing the list of primary offences by a general reference to all crimes and offences.

This amendment is in line with point (a) of Article 5(1) of the Law of 12 November 2004 on AML/CFT as the requirement to report suspicious transactions continues to apply without the obligation for supervised entities to determine the predicate offence.

2.6.2. Amendment and implementation of the AML/CFT Law

The Law of 6 February 2025 amends in particular the Law of 12 November 2004 on AML/CFT to take into account the new framework applicable to crypto-asset service providers implementing Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets and Regulation (EU) 2023/1113 of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets. Specific provisions applicable to transfers of crypto-assets directed to or originating from a self-hosted address have been introduced in the new Article 7-1a.

The Grand-ducal Regulation of 11 June 2025 implements the new Article 9-1c of the Law of 12 November 2004 on AML/CFT and details the composition and functioning of the ML/TF Prevention Committee in charge of national coordination. This committee, of which the CSSF is a member, fosters multi-disciplinary exchanges and contributes notably to the development, coordination and assessment of the national policies and strategies relating to the prevention of money laundering and terrorist financing.

2.6.3. Beneficial Owners Register (RBE, *Registre des bénéficiaires effectifs*)

The Law of 13 January 2019 establishing a Beneficial Owners Register and the Grand-ducal Regulation of 15 February 2019 on the registration, payment of administrative fees and access to information recorded in the Beneficial Owners Register were amended in 2025 to implement significant changes, notably those related to the new data control powers of the manager, the implementing procedures for granting access, the establishment of a consultative commission, the future interconnection of the RBE with the registers established by the other Member States via the European central platform, and the protection of data held in the registers.

2.6.4. Adoption of the 3rd National Risk Assessment

On 26 May 2025, the Ministry of Justice adopted the public document on the update of the National Risk Assessment (the first version of which was published in 2020) relating only to the aspects linked to money laundering risk. Indeed, from now on, terrorist financing risk will be the subject of a separate document, enabling greater granularity of the studies according to the type of risk. The financial sector remains heavily exposed to ML risk.

2.6.5. CSSF News

In addition to the circulars or press releases/communiqués mentioned above, the CSSF adopted several other documents in relation to AML/CFT in 2025:

- Circular CSSF 25/879 on the adoption of the EBA Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 ("Travel Rule Guidelines")
- Circular CSSF 25/878 on the adoption of the revised EBA guidelines on money laundering and terrorist financing risk factors;
- Circular CSSF 25/870 amending Circular CSSF 24/853 on the revised long form report for investment firms;
- the publication of a thematic review on counter-proliferation financing and the measures implemented by several investment fund managers;
- the update of several forms relating to the identification of the compliance officer in charge of the control of compliance with the AML/CFT professional obligations or of the person responsible for compliance with the AML/CFT professional obligations in the investment funds sector; and
- as regards risk assessment, the publication of the second update of its ML/TF Sub-sector Risk Assessment for the collective investment sector in February 2025.

2.7. Focus on financial restrictive measures/financial sanctions

The year 2025 was also marked by a number of major events at both EU and international level. Thus, the Council of the European Union had to adopt several important regulations to protect the Member States, their interests, their core values and their security from conflicts and wars around the world.

First, it adopted four rounds of additional sanctions against Russia, resulting in a total number of 19 sanctions in 2025, with a dynamic that corresponds to a set of closely successive financial sanctions packages, characterised by an almost quarterly frequency.

In 2025, a certain number of measures were taken, mainly concerning anti-circumvention measures, the extraterritorial extension of certain measures and the effectiveness of their implementation. The main measures included a transaction ban on credit or financial institutions established outside Russia that use the "System for Transfer of Financial Messages", a ban on engagement by EU operators with the Russian national payment card system ("Mir") or the faster payments system ("SBP"), the legal reinforcement of the concepts of "owning" and "controlling" a legal person, measures targeting also crypto-asset service providers, export restrictions on dual-use goods and technologies intended for companies located in third countries, restrictions on the provision of AI services, etc.

The sanctions against Belarus largely mirror the measures adopted against Russia.

In addition to these restrictive measures regimes against Russia and Belarus, the EU updated the financial sanctions regimes against other countries like Syria, Venezuela, Libya, the Central African Republic and Haiti, notably in view of the persistent gravity of the human rights situation in these countries, and the absence of democracy and the rule of law.

In 2025, cybercrime and, more broadly, the government- or paragovernment-led cyberattacks were also part of the EU Council's discussions and led to targeted restrictive measures with the aim of deterring and responding to major cyber-attacks which represent an external threat to the EU or its Member States. The list of persons subject to restrictive measures was updated twice in 2025.

In the year 2025, the sanctions on Iran were reintroduced. They had been suspended with the entry into force of the Joint Plan of Action (JCPoA or Iran nuclear deal) in 2015. This decision was taken following the UN Security Council's decision not to extend the lifting of sanctions on Iran. The measures reintroduced since September 2025 include those adopted by the UN Security Council since 2006 with successive UNSC resolutions and automatically transposed into EU law, and EU autonomous measures such as: asset freezes for the individuals and entities concerned, the prohibition on making funds or economic resources available to them and or also economic and financial sanctions covering the trade, financial and transport sectors. The EU also reimposed the freezing of assets of the Central Bank of Iran and of major Iranian commercial banks.

Finally, a number of specific restrictive measures against persons and entities in the context of the fight against terrorism were adopted, through which the Council of the EU intends to target leading members of EU-listed groups and entities that play a key role in planning, facilitating, preparing or perpetrating terrorist acts, including through their participation in financing or their involvement in terrorist training and recruitment. It should be noted that the EU Terrorist List (based on Regulation 2580/2001/EU) is separate from the list against those who support, facilitate or enable violent actions by Hamas and the Palestinian Islamic Jihad or from the list transposing the UN Security Council resolutions and targeting Al-Qaida and ISIL/Da'esh.

In relation to all the regulations and implementing regulations adopted across sectors during 2025, the Council reiterated that the circumvention of restrictive measures is prohibited, including attempts to circumvent them.

In this respect, Directive (EU) 2024/1226 of 24 April 2024, adopted by the European Parliament and the Council, represented a major step in the fight against the circumvention of financial sanctions by criminalising circumvention and circumvention attempts, while aiming to harmonise criminal laws at EU level in both the definition of the offences and the applicable sanctions. Financial sanctions will thus no longer be a compliance issue but a criminal risk. In view of the amendment of the Law of 19 December 2020 on the implementation of restrictive measures in financial matters, a draft law was deposited with the Chamber of Deputies in July 2025.

On this topic, the CSSF also adopted the EBA Guidelines through Circular CSSF 25/896. Taking into account the numerous developments in this area throughout 2025, the CSSF updated its FAQs on international financial sanctions.

Finally, the FATF reiterated the importance of an efficient fight against the proliferation financing at global level and underlined the need to reinforce the efficiency of national measures and international cooperation with the aim of preventing the circumvention of sanctions and the use of virtual assets for this purpose. As major deficiencies were identified in the global response to these issues, the FATF published a report specifying the methods and techniques used by those who try to circumvent the sanctions (cf. also point 2.4.2. above).

All the relevant documentation is available on the CSSF website at: https://www.cssf.lu/en/international-financial-sanctions/.

2.8. Fight against corruption at EU level and in Luxembourg

In 2023, the European Commission presented a package of anti-corruption measures which included a proposal for a directive which defined corruption as a particularly serious crime with a cross-border dimension. In December 2025, a provisional agreement was concluded on this very first anti-corruption directive, which was followed by a formal agreement in April 2026. The object of this directive, published on 11 May 2026 in the Official Journal of the European Union[5] , is to harmonise criminal legislation and strengthen the efforts to prevent, combat, prosecute and sanction corruption offences throughout the European Union.

Under this directive, active and passive bribery constitute criminal offences in both the private and public sectors. The directive covers misappropriation by public officials. It also deals with obstruction of justice by prohibiting any action aimed at interfering with the giving of testimony or with the exercise of public functions in corruption procedures.

At national level, the CSSF actively contributes to the Committee on the Prevention of Corruption (COPRECO), established by the Law of 1 August 2007 approving the United Nations Convention against Corruption of 31 October 2003. This Committee assists the government in combating corruption and contributes to the coordination of the implementation of the measures adopted within the public administration. In its AML/CFT internal strategy for 2025-2027, the CSSF identified bribery as one of the predicate ML offences requiring specific attention, in line with the high ML risk assessment associated with this predicate offence, as reiterated in the 2025 National Risk Assessment mentioned above. The CSSF thus intensified its awareness-raising activities on corruption risk and will pursue these efforts. For instance, a meeting of the public-private partnership between the CSSF, the ABBL and the FIU (which published an analysis on this matter on its website in 2026) was dedicated to this topic. Also, certain sub-sectoral risk analyses of the CSSF include sections dedicated to combating bribery as well as indicators and specific case studies to help professionals detect such offences, notably active corruption, more efficiently.

5 https://eur-lex.europa.eu/eli/dir/2026/1021/oj/eng

3. AML/CFT cooperation at national level

In addition to its bilateral exchanges with other competent authorities, including the FIU, the CAA and the Administration de l'enregistrement, des domaines et de la TVA, as well as with certain AML/CFT self-regulatory bodies, the CSSF was particularly involved, throughout 2025, in the work of the ML/TF Prevention Committee and its working groups, the above-mentioned COPRECO and the Monitoring Committee regarding financial sanctions, notably by contributing to the conduct of risk analyses in these contexts.

Successful financial crime prevention relies on the contribution of all the players, whether public or private. Every effort is essential, and prevention starts with the detection of natural or legal persons that provide illicit financial sector activities, i.e. the provision of financial services without approval or registration, or without the legally required authorisation. Any detected illicit activities must be reported to the competent authorities (prosecution offices, police and/ or the CSSF) in order to guarantee and preserve the integrity of the financial system and to protect users in an environment of ever-increasing frauds and scams. To this end, warnings are updated and published by the CSSF on its website.

Commission de Surveillance du Secteur Financier

283, route d'Arlon
L-2991 Luxembourg
Tel.: (+352) 26 251-1
Email: direction@cssf.lu
Website: www.cssf.lu

Design: binsfeld
Printed in Luxembourg by Imprimerie Centrale

Commission de Surveillance
du Secteur Financier

283, route d'Arlon
L-2991 LUXEMBOURG