EBA/Op/2025/10

28 July 2025

Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector

Introduction and legal basis

1. The EBA's competence to deliver an Opinion on money laundering (ML) and terrorist financing (TF) risks affecting the EU's financial sector is based on Article 6(5) of Directive (EU) 2015/849([1]), which requires the EBA to issue such an Opinion every two years.

2. This Opinion is addressed to the European co-legislators and AML/CFT competent authorities. It serves to inform competent authorities' application of the risk-based approach to AML/CFT supervision and the European Commission's Supranational Risk Assessment.

3. This is the EBA's fifth Opinion on ML/TF risks. It is based on data from January 2022 to December 2024, including 52 AML/CFT competent authorities' responses to the EBA's biennial ML/TF risk assessment questionnaire, submissions to the EBA's EuReCA database and findings from the EBA's ongoing work to lead, coordinate and monitor the EU financial sector's fight against ML/TF.

4. The EBA has not conducted an open public consultation or carried out a cost-benefit analysis and has not requested advice from the Banking Stakeholder Group because the proposals made to competent authorities and the co-legislators in this Opinion build on existing regulations and guidelines.

General comments

5. Since the EBA's fourth Opinion on ML/TF risks was published in 2023, the financial sector has faced a dynamic and increasingly complex ML/TF risk landscape. The rapid evolution of financial

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

technologies and new financial products such as crypto assets, and the growing interconnection of financial products and services across sectors, have introduced new vulnerabilities.

FinTech: innovation comes at the cost of compliance

6. The market share of FinTech firms continues to grow, driving innovation in financial services, expanding access and enhancing consumer experience. Yet 70% of competent authorities in the EU report high or increasing ML/TF risks in this sector. They are concerned that this rapid growth may not have been accompanied by robust AML/CFT controls, and that some FinTech providers may be prioritising customer acquisition over compliance. Key vulnerabilities include exposure to cybercrimes, outsourcing without effective oversight, and inadequate customer due diligence controls.

7. The EBA notes that, based on the information provided by competent authorities, many FinTech firms lack the expertise and governance structures necessary to identify and tackle ML/TF risks effectively. Competent authorities need to be mindful of this when putting together their supervisory plans to ensure compliance keeps pace with innovation in this sector. This is particularly important, since the acquisition by traditional institutions of FinTech firms means that these risks may also spill over into other sectors.

RegTech: poor implementation hampers potential for better controls

8. RegTech solutions offer significant potential for better compliance and a reduction of manual errors, but their successful deployment has been hampered by inadequate in-house expertise, poor governance and insufficient oversight. More than half of all submissions to the EBA's EuReCA database suggest that serious compliance failures were due, at least in part, to the improper use of AML/CFT RegTech. At the same time, the widespread use by financial institutions of RegTech products by a small number of providers, and off-the-shelf solutions that are not fit for purpose, exacerbate vulnerabilities, particularly in credit and payment institutions.

9. The EBA emphasises the opportunities afforded by the increasing use of technology for AML/CFT compliance purposes. To ensure their safe and prudent use, competent authorities should continue to identify and promote good practices in the use of RegTech – such as streamlining workflows, creating dynamic risk profiles and enabling institutions to manage large data volumes efficiently, while taking the steps necessary to ensure that these tools are used responsibly.

Crypto: risks remain high while transition to the new regulatory framework is underway

10. The abuse of crypto asset services for financial crime purposes remains a key area of concern. This is compounded by a surge in transaction volumes and a 2.5-fold increase in the number of authorised CASPs in the EU between 2022 and 2024. However, findings from authorities responsible for licensing and registration indicate that some entities have attempted to bypass these processes, thereby evading AML/CFT supervision. Moreover, competent authorities found that CASPs often lacked effective AML/CFT systems and controls. In several cases, concerns were also raised regarding the integrity of senior management and the transparency and adequacy of governance arrangements.

11. The EBA highlights that the lack of robust AML/CFT controls in the sector reflects a gap between regulatory expectations, legal obligations and actual practice. Enhanced supervisory coordination and enforcement, and the effective and consistent application of the new EU crypto framework, are essential to address this challenge.

Fraud: risks escalate as automation and AI fuel increasingly sophisticated schemes

12. The expansion of cybercrime and fraud, driven by technological sophistication, continues to outpace the sector's defensive capabilities. Criminals use AI for money laundering to automate financial schemes, conceal fund sources, and make high-risk transactions harder to detect. Perpetrators can also use AI to generate fake documents, simulate legitimate operations and use deep-fake technologies to evade CDD measures. Financial institutions face challenges in detecting sophisticated AI-driven attacks that are increasing in both volume and velocity.

13. Addressing these threats will require advanced technologies and specialised expertise. The EBA emphasises the need for responsible AI deployment, supported by robust governance, staff training, and real-time monitoring capabilities. Institutions must remain vigilant and adaptive in this evolving threat landscape. Competent authorities have an important role to play in this regard.

Restrictive measures: compliance risks grow amid complex regimes

14. The number and complexity of EU sanctions packages continue to pose significant challenges for financial institutions, as they often cannot be implemented by using standard sanctions screening tools. Competent authorities have increased their supervisory actions, particularly focusing on the quality of screening systems and the effectiveness of measures to implement restrictive sanctions. Many institutions still lack adequate policies and procedures.

15. Additional challenges arise in the screening of SEPA instant credit transfers, which may expose PSPs to a heightened risk of breaching restrictive measures that are not targeted financial sanctions – such as sectoral sanctions. Furthermore, fragmented access to information in card payment infrastructure can lead to inadvertent breaches of restrictive measures.

16. Going forward, the EBA expects that inconsistent implementation of restrictive measures will be reduced. The EBA's two sets of guidelines, which establish the first common EU standards for financial institutions to comply with Union and national restrictive measures, will apply from the end of 2025. Under the new AML/CFT framework, AMLA and national AMLC/CFT supervisors will monitor whether obliged entities have appropriate policies and procedures in place for implementing targeted financial sanctions.

Concerted action by regulators, supervisors and institutions has contributed to improvements in priority risk areas

17. This Opinion on ML/TF risks also highlights positive developments. Risks related to tax crimes and unwarranted de-risking, which have been the EBA's focus over the last four years – appear to be decreasing overall. Eighty percent of competent authorities indicate that unwarranted de-risking is declining or is no longer an issue in their Member State.

18. Levels of supervisory engagement have increased across all sectors, with information from competent authorities highlighting a significant number of targeted and thematic inspections. The majority of AML/CFT supervisors have also provided specific guidance to ensure that expectations regarding effective AML/CFT systems and controls are properly applied. As a result, residual risk levels have been improving in the credit institutions, credit providers and the three financial market sectors in particular. Although the poor quality of controls in the payment institutions and crypto sectors – particularly among newly authorised entities – means that these controls remain insufficient to mitigate the high inherent risk levels, supervisory engagement in these sectors has also increased, which should lead to future improvements.

19. For the first time since the EBA began to issue Opinions on ML/TF risk, risks associated with products and services are overtaking risks related to firms' customers. However, 61% of breaches across all sectors are still caused by customer due diligence shortcomings.

20. Overall, while awareness of ML/TF risks is growing, the effectiveness of AML/CFT systems remains uneven. The findings underscore the need for continued regulatory clarity, and a more consistent application of risk-based approaches across the EU financial sector.

Specific comments

21. The specific comments and findings supporting the EBA's proposals are available in the Report attached to this Opinion.

This opinion will be published on the EBA's website.
Done at Paris, 28/07/2025

[signed]
[José Manuel Campa]
Chairperson
For the Board of Supervisors

European Banking Authority

REPORT

ON MONEY LAUNDERING AND TERRORIST FINANCING RISKS AFFECTING THE EU'S FINANCIAL SECTOR

EBA/REP/2025/22 JULY 2025

Contents

List of figures

Abbreviations

AMLD	Anti-Money Laundering Directive
AMLR	Anti-Money Laundering Regulation
AML	anti-money laundering
ART	asset-referenced token
CA	competent authority
CASP	crypto assets service provider
CDD	customer due diligence
CIU	collective investment undertakings
CFT	countering the financing of terrorism
EDD	enhanced due diligence
EMI	e-money institution
EMT	electronic money token
ESG	environmental, social and governance
FIU	financial intelligence unit
FTR	Funds Transfer Regulation
LEA	law enforcement authority
LIU	life insurance undertaking
LII	life insurance intermediaries
MiCA	Markets in Crypto Assets Regulation
ML	money laundering
NRA	national risk assessment
PEP	politically exposed person
PSD2	Payment Service Directive 2
PSP	payment service provider
RTS	regulatory technical standards
SEPA	single euro payments area
STR	suspicious transaction report
TF	terrorist financing
UBO	ultimate beneficial owner
vIBAN	virtual international bank account number

Executive summary

22. The EBA has been issuing Opinions on money laundering and terrorist financing (ML/TF) risk every two years since 2017. Since the first Opinion on ML/TF risk was issued, the EU's legal and institutional framework has undergone significant changes; anti-money laundering and countering the financing of terrorism (AML/CFT) supervisors have moved towards more risk-based and targeted approaches, and the opportunities and risks financial institutions face in relation to financial crime have evolved.

23. This is the EBA's fifth Opinion on ML/TF risks. It reveals a complex ML/TF risk landscape shaped by rapid technological innovation, regulatory reform, and shifting criminal behaviours. FinTech, RegTech and AI are central to these developments. Yet while innovation can help make the fight against financial crime more streamlined and effective, the EBA's findings suggest that the sector's drive for innovation and growth may be outpacing its ability to manage ML/TF risks, with firms in the credit institutions, payment institutions and e-money sectors particularly exposed. In this context, the unthinking application of AML/CFT RegTech solutions and spill-over risks resulting from the increased interconnectedness of traditional financial services providers with innovative financial services providers, such as crypto assets service providers (CASPs), are of particular concern.

24. This Opinion on ML/TF risks also highlights positive trends. According to competent authorities, risks associated with tax crime appear to have reduced overall, and unwarranted de-risking has decreased. At the same time, residual risk levels have been improving thanks to better supervision and more effective AML/CFT systems and controls in the credit institutions, investment funds and life insurance sectors in particular. For the first time, therefore, products and services risks are outpacing residual risks related to firms' customers. By contrast, inherent and residual risk levels have increased in the payment institutions, e-money and crypto sectors, and TF risk remains under-addressed.

25. The EBA's findings underscore the need for regulatory clarity and a more consistent application of risk-based approaches across the EU financial sector. This will be particularly important as legal and regulatory changes resulting from the new EU AML/CFT package take effect.

1. Background and legal basis

26. The EBA's competence to deliver an Opinion on ML and TF risks affecting the EU's financial sector is based on Article 6(5) of Directive (EU) 2015/849([2]), which requires the EBA to issue such an Opinion every two years.

27. This Opinion is addressed to the European co-legislators and AML/CFT competent authorities. It serves to inform competent authorities' application of the risk-based approach to AML/CFT supervision and the European Commission's Supranational Risk Assessment.

[2] And Articles 16a(1) and 29(1)(a) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

2. Methodology

28. This the EBA's fifth Opinion on ML/TF risks is based on data from January 2022 to December 2024. It draws on the following information sources:

- Responses to a questionnaire that was sent to the 58 competent authorities (CAs) that are responsible for the AML/CFT supervision of institutions within the EBA's AML/CFT remit. The questionnaire covered ML/TF risks and supervisory activities from January 2022 to December 2024. In total, 52 CAs from 29 Member States and EEA countries responded to this questionnaire;
- Submissions to EuReCA, the EBA's AML/CFT database([3]);
- Findings from the EBA's reviews of CAs' approaches to AML/CFT supervision([4]);
- Findings from the EBA's work on supervisory colleges([5]);
- Findings from the EBA's peer reviews;
- Findings from the EBA's regulatory and wider risk assessment work;
- Information provided by members of the EBA's permanent internal committee on anti-money laundering and countering terrorist financing (AMLSC), which it established pursuant to Article 9a(7) of Regulation (EU) No 1093/2010.

29. As was the case in previous Opinions on ML/TF risks, the EBA analysed these data using a combination of data analytics software and qualitative assessments. In accordance with Article 14(7) of the Rules of Procedure of the Board of Supervisors([6]), the EBA's Board of Supervisors approved this Opinion.

[3] EuReCA, the EBA's AML/CFT database.

[4] EBA/REP/2024/25.

[5] EBA/REP/2024/27.

[6] Decision of the European Banking Authority of 22 January 2020 concerning the Rules of Procedure of the Board of Supervisors (EBA/DC/2020/307 (consolidated version)).

3. Cross-sectoral ML/TF risks

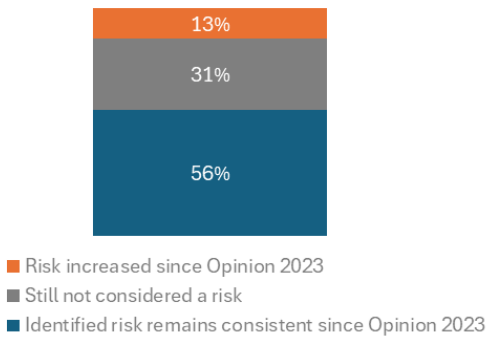
30. The rapid growth of FinTech, crypto assets and interconnected financial services has introduced new vulnerabilities. A focus on customer acquisition over compliance, and careless RegTech deployment, have heightened exposure to ML and TF threats. Meanwhile, risks associated with cybercrime, fraud, corruption, sanctions evasion and TF may not be managed effectively, with many institutions still lacking robust risk assessment and monitoring frameworks.

3.1. FinTech firms appear to prioritise growth over compliance

31. **FinTech products and services, i.e. technologically enabled financial innovations, are becoming more widespread and mainstream**. This is due in part to an increase in the number of authorised e-money institutions that are, historically, among the main providers of FinTech products and services. It is also due to the introduction of new innovative products and services, the increasing offering of such products and services by traditional financial services institutions and a related, upward, trend of mergers and acquisitions by credit institutions of FinTech companies.

32. **At the same time, information provided by CAs suggests that a gap exists, and may be increasing, between the evolving FinTech landscape and the effectiveness of FinTech providers' AML/CFT systems and controls.** CAs point to high inherent ML/TF risks linked to the design and functionality of many FinTech products and services. Sixty-four percent of CAs (up from 39% in 2023) highlight exposure to cybercrime, including cyber-enabled fraud, as an important vulnerability, 55% of CAs point to complex internal arrangements such as widespread reliance on outsourced services provision as a significant or very significant ML/TF risk, and 86% of CAs consider the risk associated with cross-border transactions to be significant or very significant. By contrast, almost half of all CAs assess the AML/CFT controls institutions put in place in this regard as inadequate, with transaction monitoring (52% of CAs), customer due diligence (CDD) measures (48% of CAs, up from 34% in 2023) and an overall lack of understanding by institutions of ML/TF risks associated with their FinTech products and services a particular concern (52% of CAs, up from 35% in 2023). In total, 69% of CAs consider that the level of ML/TF risk associated with FinTech has remained high or has increased.

Figure 1: Evolution of risk compared to the risks identified in the 2023 Opinion – FinTech



33. **In the current competitive environment, technology-focused firms appear to prioritise rapid growth over AML/CFT compliance.** In addition to information provided by CAs, this assessment reflects findings in Section 3.3. of this report and those from the EBA's 2024 report on the functioning of AML/CFT Colleges([7]). A thematic review of a small number of AML/CFT colleges for FinTech firms found that the number of staff was often insufficient to handle the alerts generated by the screening and monitoring tools. In some cases, staff members were not sufficiently skilled or knowledgeable to properly analyse the alerts generated by the tools. Firms that were growing at a fast rate appeared to be particularly exposed to both issues.

3.2. White labelling creates challenges in terms of third-party oversight and AML/CFT supervision

34. **White labelling refers to a firm (the *partner*) offering the financial products and services of a licensed financial institution (the *provider*) under its own brand.** The partner may not itself be a financial institution or obliged entity. AML/CFT obligations, including CDD, will be discharged through outsourcing arrangements or, where the provider is an obliged entity, reliance agreements. Irrespective of the contractual arrangements between providers and partners, providers remain ultimately responsible for compliance with their AML/CFT obligations.

35. **Ninety percent of CAs who currently assess the ML/TF risks associated with white labelling rate these risks as medium or high.** However, nearly half of all CAs do not assess this risk, or assess it as low because in their Member State white labelling is limited in scale or confined to low-risk products such as low-value prepaid cards or basic payment services.

36. **The ML/TF risks associated with white labelling stem from the complexity of the contractual arrangements, the distribution of financial services products by entities that may not be obliged entities themselves, and the cross-border nature of many such services.** This can make it challenging for providers to integrate these products and their corresponding risks into their AML/CFT framework, and to adequately monitor and control the ML/TF risks arising from these services([8]). CAs also noted risks related to virtual international bank account numbers (vIBANs), including fraud and transaction obfuscation.

37. **CAs may be unaware of the extent of white labelling in their Member State.** White labelling agreements may not need to be notified to supervisory authorities unless they meet certain thresholds or conditions, such as involving agency under PSD2 or constituting a material change to the business model. As a result, CAs may not know how services are delivered to customers, particularly when such services are bundled with non-regulated offerings or delivered across borders. This may hamper CAs' ability to monitor compliance, ensure effective supervision, and detect emerging risks.

38. **The EBA is currently assessing the risks associated with white labelling** from a prudential, consumer protection and financial crime perspective. The report will be published in Q3, 2025.

[7] EBA/REP/2024/27.

[8] Add reference if report published before the Opinion, otherwise delete.

3.3. Risks and challenges associated with virtual IBANs

39. In May 2024, the EBA published a report on virtual IBANs([9]), identifying ML/TF risks stemming from lack of visibility of the identity of the end users of vIBANs, creating challenges for payment service providers (PSPs) in monitoring their business relationships and their customers' transactions and challenges for financial intelligence units (FIUs) and law enforcement authorities in tracing suspicious transactions involving vIBANs. The EBA also observed divergent interpretations across CAs about the features and definition of vIBANs, and about the definition of an IBAN in the SEPA Regulation and in the ISO IBAN standard, and highlighted the risk of vIBANs being used by non-EU financial institutions or by EU non-PSPs to provide payment services without the required authorisation.

40. In line with this assessment, CAs consider that the risk associated with vIBANs is high for PIs and CIs, though the nature of the risk varies by sector. Almost a quarter of CAs for PIs highlight that vIBANs can obscure the true identity of account holders, whereas CAs of credit institutions are more concerned about the difficulty in distinguishing between payments received through virtual and traditional current accounts. For both sectors, CAs consider the risk of cascading vIBANs – where a PSP provides its customers with vIBANs generated by another institution for use in payment transactions or for further transfer to its customers (also known as reissuing) – as very significant. Another notable risk arises in cases where the master account is held in a different MS from that of the end customer and where a vIBAN contains a different country code from the IBAN of the master account. These divergent approaches create a risk of supervisory gaps and risks of regulatory arbitrage.

41. **A definition of vIBANs has been included in the AML Regulation([10]), which will apply from 10 July 2027.** The AMLR also introduces a mitigating measure for ML/TF risks associated with the lack of transparency of vIBANs, by requiring that vIBANs be registered in national central registers of bank accounts. The proposed regulatory technical standards([11]) under Article 28 of AMLR recommend the identification and verification of the identity of the natural or legal persons using a virtual IBAN.

3.4. The unthinking use of RegTech creates ML/TF risks

42. **RegTech, i.e. any range of applications of technology-enabled innovation for regulatory, compliance and reporting requirements, offers significant benefits in the fight against financial crime**. It can help streamline workflows, create dynamic risk profiles and enable institutions to manage large data volumes efficiently. It also offers the potential for institutions to share data safely and securely. Twenty-nine percent of CAs identified good practices in this regard.

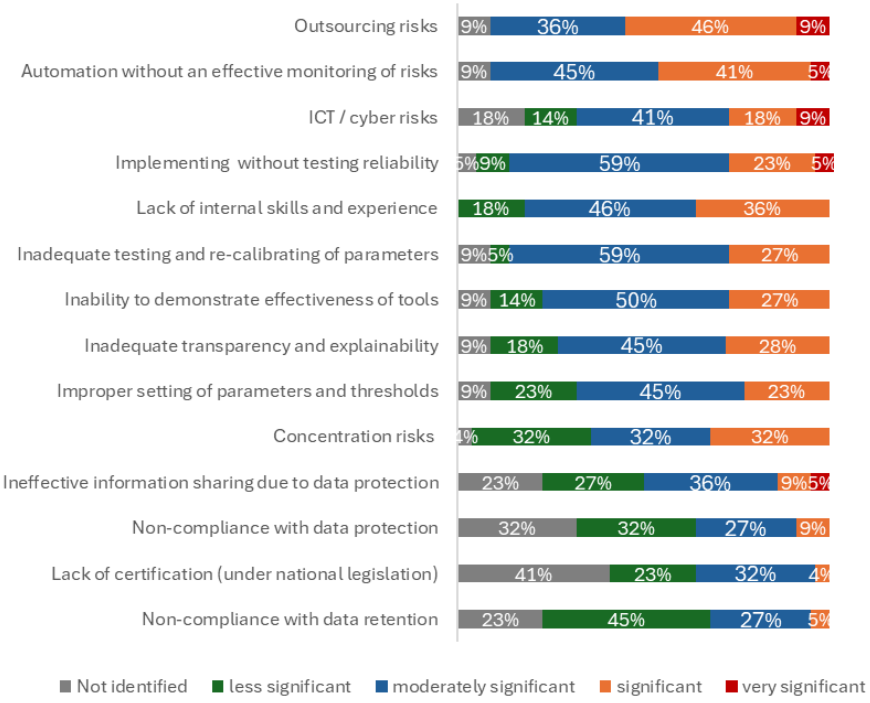
43. **Nevertheless, half of all CAs surveyed for this Opinion identified ML/TF risks associated with the use of RegTech solutions by obliged entities, and 15% consider that the risk has increased.**

[9] EBA/Rep/2024/08.

[10] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[11] EBA/CP/2025/04.

Figure 3: Types of risks identified in relation to RegTech



44. **Outsourcing, automation without effective monitoring, and lack of in-house skills and experience are the three most significant ML/TF risks identified by CAs in relation to RegTech.**

- More than half of all CAs (55%) consider that outsourcing of RegTech poses a significant or very significant risk. CAs were particularly concerned about the adequacy of institutions' oversight of large-scale outsourcing arrangements in the credit institutions, credit providers, payment institutions and e-money institutions sectors.

- Forty-six percent of all CAs assess risks related to the use of automated solutions without adequate safeguards as significant or very significant across the credit institutions, e-money institutions, crypto asset service providers, credit providers, life insurance undertakings and life insurance intermediaries sectors.

- Relatedly, one third of CAs point to significant risks associated with institutions implementing RegTech solutions without adequate testing, failing to ensure the transparency and explainability of RegTech systems, and being unable to demonstrate the effectiveness of RegTech systems and tools.

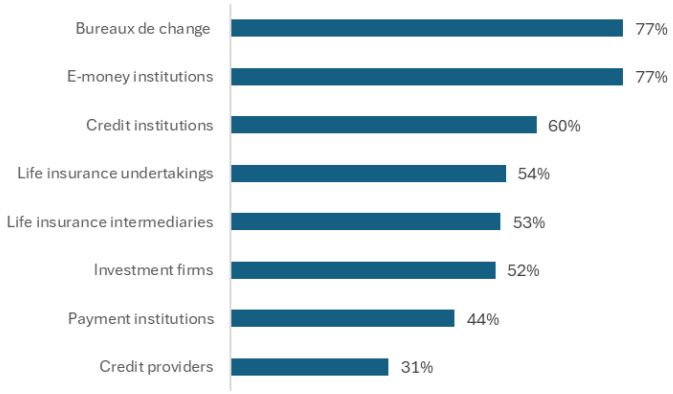
- Thirty-six percent of CAs indicate that institutions across all sectors lack the in-house skills and experience necessary to ensure effective use of RegTech solutions.

45. **Thirty-two percent of CAs view concentration risks as significant**, as relying heavily on a small number of RegTech solutions across many supervised entities can create systemic vulnerabilities – especially if those solutions are not customised to each entity's specific needs.

46. **Failure to ensure that RegTech solutions are fit for purpose can be serious**: more than one third of CAs point to significant or very significant risks linked to the unthinking use of onboarding and CDD, transaction monitoring and screening RegTech solutions. Data from EuReCA suggest

that, over the course of 2023 and 2024, in more than half of the total number of financial institutions for whom reports were submitted, CAs identified a total of 277 material weaknesses linked to issues involving RegTech technologies, systems and tools.

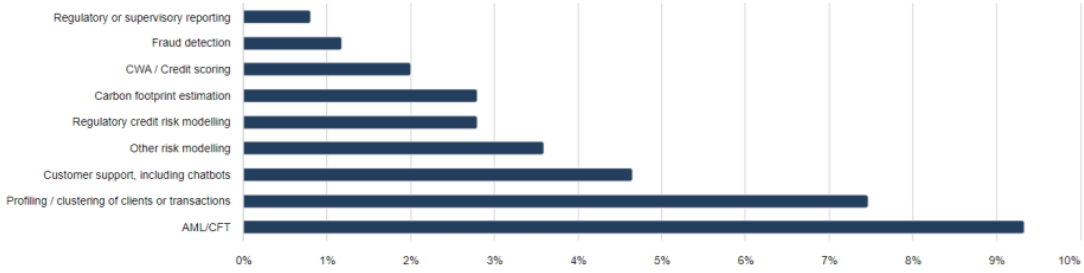
Figure 4: Percentage of financial institutions with material weaknesses reported to EuReCA linked to the use of technologies within their sector



Box 1. Use of Artificial Intelligence

The EBA Risk Assessment Report – Autumn 2024([12]) suggests that the adoption of General Purpose Artificial Intelligence (GPAI) in the EU banking sector is still at an early stage, with banks mostly testing and experimenting with GPAI via proof-of-concepts or a sandbox approach. Around 10% of EU banks are already testing the use of GPAI for many other use cases, such as those related to AML/CFT and to the profiling and clustering of clients and transactions.

Figure 5: Proportion of banks testing GPAI, but still not using it in production, per use case, autumn 2024



Source: EBA Risk Assessment Questionnaire

CAs that responded to the ML/TF risk assessment questionnaire observed that financial institutions face challenges in understanding AI technologies and in recruiting skilled staff, particularly as they attempt to integrate AI and machine learning into AML/CFT processes. These challenges could compromise the quality of AML/CFT efforts. Risks were identified in the following sectors: credit institutions, e-money institutions, life insurance undertakings and life insurance intermediaries.

Meanwhile, criminals use AI for money laundering to automate financial schemes, conceal fund sources, and make high-risk transactions harder to detect. Perpetrators can also use AI to generate fake documents, simulate legitimate operations and use deep-fake technologies to evade AML/CFT measures like identity control. Financial institutions face challenges in detecting sophisticated AI-

[12] Risk Assessment Report of the European Banking Authority, November 2024.

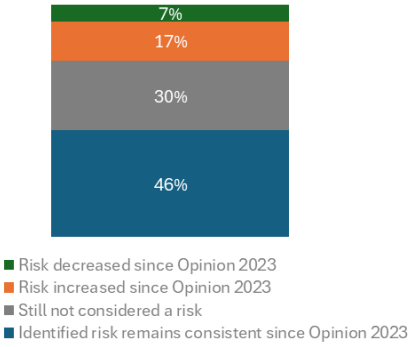
driven attacks that are increasing in both volume and velocity. Addressing these threats will require advanced technologies and specialised expertise.

Please refer to Section 3.10.

3.5. Concerns remain around CASPs' ability to identify and manage ML/TF risk while volumes of transactions soar

47. **Between 2022 and 2024, the number of licensed or registered CASPs([13]) has multiplied by 2.5 to reach 2 525 at the end of 2024, as has the volume and average value of crypto transactions.** As a result, 17% of CAs consider that the risks related to crypto assets service provision has increased.

Figure 6: Evolution of risk compared to the risks identified in the 2023 Opinion – Crypto assets

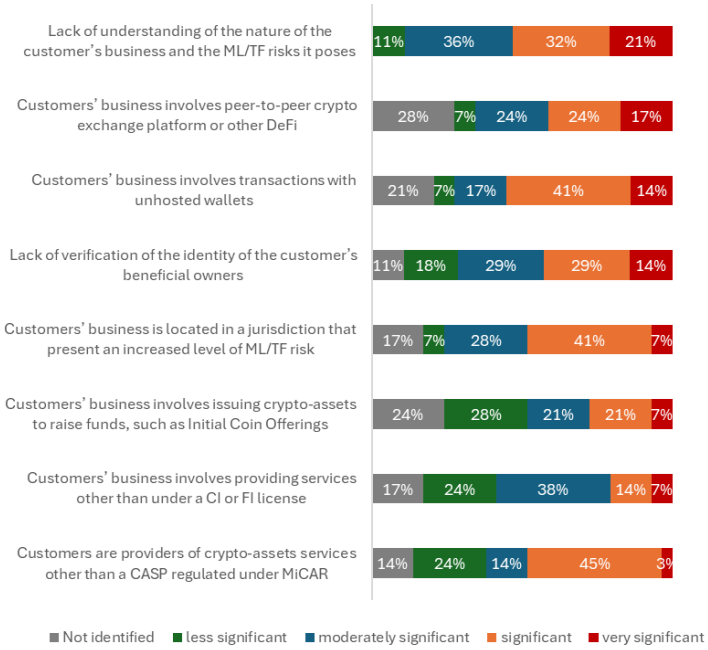


48. **At the same time, 7% of CAs considered that the ML/TF risk has decreased, as CASPs are updating their systems and controls in preparation for the application of the FTR and MiCA([14]).** They noted that some CASPs appeared to be pausing new activities in the intervening time.

[13] This section is based on data collected from January 2022 to December 2024, prior to the entry into force of MiCA and the FTR in December 2024. Accordingly, in this report, the term 'CASP' does not refer to crypto asset service providers as defined in Article 3(1)(16) MiCA. Instead, it refers to entities that provided crypto asset services in accordance with applicable law before 30 December 2024, and which may continue to do so either until the end of any transitional period established under national law (if applicable), or until they are granted or denied authorisation pursuant to Article 63 – whichever occurs first.

[14] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

Figure 7: Types of risks identified in relation to crypto assets



49. **CAs that carried out inspections of CASPs point to significant AML/CFT systems and controls deficiencies that appear to be prevalent across the sector.** The most significant risk remains the lack of understanding of the ML/TF risks associated with individual business relationships, with 53% of CAs assessing this risk as very significant or significant. This is particularly concerning, as more than half of CAs identify high risks associated with the location of the customer or their business activity. Lack of oversight and control is another contributing factor, while 43% of CAS point to significant risks linked to the failure by CASPs to ensure adequate verification of their customers' or beneficial owners' identity.

Box 2. Learning lessons from CASP supervision

In 2024, the EBA conducted an exercise on the lessons learned from the EU AML/CFT supervisory measures towards specific crypto assets entities and the impact on the wider EU sector. Findings from CAs in charge of licensing/registration suggest that some entities have sought to bypass that step, thereby avoiding AML/CFT supervision. In addition, findings from competent authorities suggest that many CASPs did not have effective AML/CFT systems and controls in place. Furthermore, in several cases, the integrity of CASPs' senior management and the transparency and adequacy of the governance arrangements were not assured. This suggests that, overall, the ML/TF risk in the sector may not have been identified or managed adequately in all cases.

50. **CASPs and the provision of other financial services are increasingly interlinked, particularly in the credit institutions, payment institutions and e-money institutions sectors.** This means that ML/TF risks affecting CASPs are also spilling over into other sectors. For example, 35% of CAs observed an increasing crossover in services between CASPs and e-money institution (EMIs), and CASPs and PIs for the conversion of cryptocurrency to fiat currency and vice versa. Crypto-to-fiat services offered through group structure arrangements based on outsourcing often leads to unclear governance and operational boundaries. One CA noted the risk posed by high-value goods dealers accepting hybrid electronic payment methods, such as foreign payment methods or prepaid cards linked to an e-wallet with cryptocurrency balances.

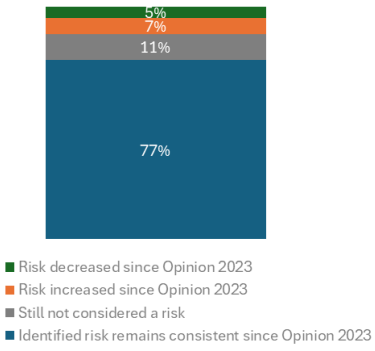
51. **CAs of CASPs, CIUs and fund managers have reported a rise in fraud targeting investors in crypto assets**, notably 'rug pull scams', where fake tokens lure investors before the creators vanish with the funds. Risks increase when fund managers invest in crypto assets without sufficiently testing the new products like NFTs and DeFi, often without verifying the source of crypto-derived funds. Additional concerns include issuing crypto assets to raise funds – such as unregulated token sales via decentralised platforms, which can lead to fraud and regulatory breaches. These issues underscore the need for strong due diligence, ongoing oversight and clear regulatory frameworks.

52. **The new EU crypto framework applies from the end of 2024**. It introduces four key AML/CFT rules for CASPs. The EBA has built a common approach([15]) to tackling ML/TF risks in this sector, with 14 regulatory instruments to institutions and their supervisors that specify how the new rules should be applied at market entry and throughout the life cycle of a CASP, EMT or ART.

3.6. Exposure to terrorist financing risks remain constant while the use of stablecoins for TF purposes increases

53. **According to CAs, the level of TF risk remains stable overall, and the observations set out in the 2023 Opinion remain relevant.** Four CAs consider that the risk has increased because of a change in neighbouring countries' geopolitical situation, an increase in violent right-wing extremism or terrorism due to increased influxes of refugees related to armed conflicts. Two CAs say that the risk has decreased because of growing awareness by institutions of TF risks and better monitoring systems, especially in large financial institutions. Europol's annual EU Terrorism Situation and Trend Report([16]) (TE-SAT) concurs with those findings.

Figure 8: Evolution of risk compared to the risks identified in the Opinion 2023 – Terrorist financing



54. **Investigations by law enforcement authorities across Member States show that cryptocurrencies continue to be used as a means of transfer for terrorism financing.** However, a shift away from the prevalent use of Bitcoins towards stablecoins was observed by Europol.

Box 3. E-money tokens and ML/TF risks

By the end of 2024, there were 13 issuers of e-money tokens (EMTs) in the EU. According to CAs, the risks associated with the use of EMTs are multifaceted and significant. One major risk is

[15] Preventing money laundering and terrorism financing in the EU's crypto assets sector.

[16] European Union Terrorism Situation and Trend Report 2024.

the potential for illicit funds to be converted into EMTs to obfuscate the source of funds. The lack of transparency in secondary markets – such as those facilitated through peer-to-peer (P2P) platforms – where Know Your Customer (KYC) requirements are not consistently enforced, exacerbates this issue. Conversions can occur without proper scrutiny, leading to illicit funds being integrated into the financial system.

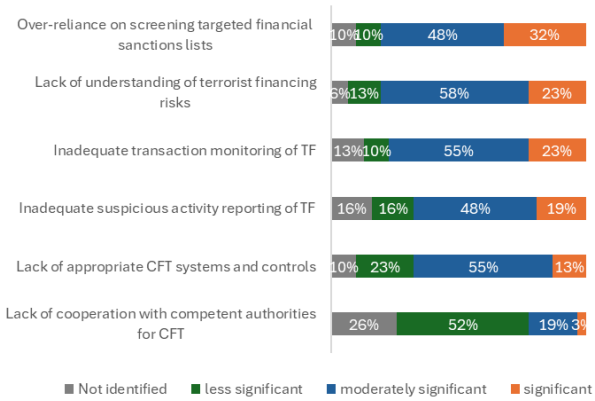
This risk increases when individuals use self-hosted wallets for peer-to-peer transactions, operating outside of the traditional financial ecosystem and not subject to standard CDD. Transactions involving foreign entities with lower regulatory standards further undermine traceability. Once EMTs are acquired, they may be redeemed for fiat currency, making it difficult for authorities to trace the financial trail, particularly when such tokens are circulated outside regulated environments.

The use of stablecoins, including EMTs, is increasingly attractive to cybercriminals due to their relative price stability, often being pegged to popular currencies like the dollar or euro, and their usability for international transfers. This makes them useful for activities such as TF, money laundering, sanctions evasion, and ransomware payments.

Additionally, where EMT issuers are designated as 'gatekeepers' under the Digital Markets Act (DMA) (Regulation (EU) 2022/1925), their control over essential digital services may pose systemic risks and complicate the oversight and enforcement of AML/CFT obligations.

MiCA applies from 31 December 2024, or later if the transition period applies. Issuers of EMTs must be authorised as credit institutions or e-money institutions and comply with requirements set out in MiCA to operate in the EU. After obtaining that authorisation, all CASPs and issuers of EMTs have to ensure compliance with EU AML/CFT rules. This includes assessing and understanding the ML/TF risk to which they are exposed, and putting in place internal policies, controls and procedures that are adequate and commensurate to that risk, following the various EBA Guidelines([17]).

Figure 9: Types of risks identified in relation to systems and controls for countering terrorist financing



55. **One third of all CAs were concerned that TF risks were insufficiently managed across all sectors.** They pointed to institutions over-relying on screening targeted financial sanctions lists as the only TF monitoring tool. The lack of understanding of TF risks represents a significant level of risk for 23% of CAs. These figures reflect data in EuReCA: between 2022 and 2024, 62 material weaknesses related to TF risk. Of these:

[17] Preventing money laundering and terrorism financing in the EU's crypto assets sector.

- Almost half involved the lack of a sufficiently robust methodology for assessing TF risks. In those cases, financial institutions did not distinguish between ML and TF risks in their business-wide risk assessments, or did so inadequately.

- Thirty-eight percent involved the absence of transaction monitoring scenarios or failures in the transaction monitoring systems to detect TF. For example, institutions offering products with a significant exposure to TF risks failed to consider low amounts or to screen for adverse public information that may affect the risk profile of customers, particularly those with convictions for acts connected to terrorism.

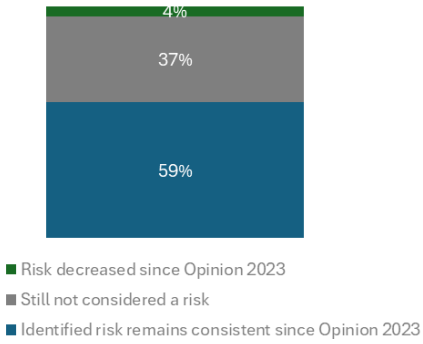
- Thirty-five percent of TF weaknesses were linked to deficiencies in sanctions screening tools for entities designated for terrorism or TF reasons.

56. **In December 2024 the EBA published a factsheet on countering TF risk([18])**. It emphasises the difference between targeted financial sanctions against terrorism and the detection of TF, and why detection is just as, if not more, important than targeted sanctions. The factsheet also lists all EBA Guidelines that contain guidance on the steps financial institutions and their supervisors should take to make sure that controls to counter TF are effective.

3.7. ML/TF risks related to tax-related crimes are perceived as decreasing by some CAs, due to legislative changes and enhanced compliance efforts

57. **In most MS, the risks related to the laundering of proceeds from tax crimes have remained constant since the 2023 Opinion was published.** The portion of CAs who do not consider that laundering the proceeds of tax crime is a risk in their jurisdiction has increased from 20% to 37% during that period. No CAs noted an increase in tax-related crimes, and two CAs indicated that the risk had decreased as a result of legislative change or the provision of regulatory guidance. Overall, tax fraud and tax evasion are the most commonly identified tax-related crimes.

Figure 10: Evolution of risk compared to risks identified in the 2023 Opinion – Tax crimes



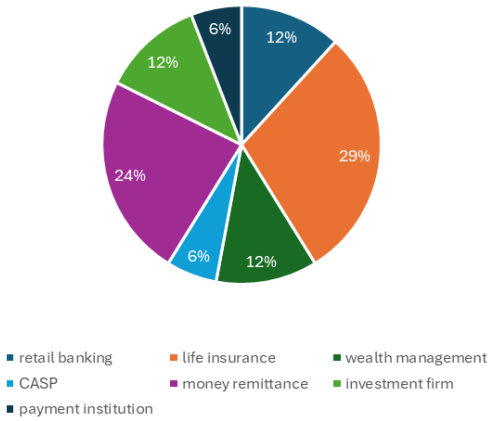
58. **Most CAs have taken concrete steps to address ML/TF risks related to tax crime in their Member State.** Most CAs added dedicated questions in their annual ML/TF risk questionnaire.

[18] Factsheet on countering terrorist financing.

Fifteen percent of CAs conducted thematic reviews or included this topic in their on-site AML/CFT inspections. In addition, 29% of CAs exchanged information on tax crime-related risks with tax authorities or provided training to financial institutions. Forty-three percent of Member States included exposure to tax-related crimes in their updated national risk assessment or their sectoral risk assessment.

59. **CAs reported 39 material weaknesses involving tax-related crimes to EuReCA between 2022 and 2024.** These weaknesses were prevalent in the life insurance and money remittance sectors, followed by wealth management, investment firms and retail banking.

Figure 11: Tax-related crime material weaknesses by sectors



60. **In February 2025, the EBA published a Peer review on tax integrity and dividend arbitrage schemes([19]).** It reviewed whether AML/CFT supervisors' supervisory activities are commensurate with the level of tax crimes in their MSs. The EBA found that most of the supervisors within the scope of this review largely or fully applied the benchmarks assessed, and hence supervised these areas well overall. The EBA identified general and individual follow-up measures, which will help further build consistency and effectiveness in supervisory outcomes across the EU and limit the financial system's exposure to illegal tax schemes and other tax evasion.

3.8 Material weaknesses in relations to PEPs continue, while corruption in the financial sector is insufficiently addressed

61. **Risks associated with Politically Exposed Persons (PEPs)** remain consistent for almost 75% of CAs. Exposure to PEPs from other EU/EEA jurisdictions remains a concern for 30% of CAs. Eighteen percent of CAs point to concerns about the application of enhanced due diligence (EDD) measures to business relationships involving PEPs. Between 2022 and 2024, 203 material weaknesses in EuReCA related to PEPs, mainly in the investment firms sector, followed by life insurance undertakings, bureaux de change and credit institutions. The use of cryptocurrencies or FinTech to transfer bribes is a rising trend.

[19] EBA/REP/2025/05.

Figure 12: Evolution of risk compared to the risks identified in the Opinion 2023 – Corruption and PEPs

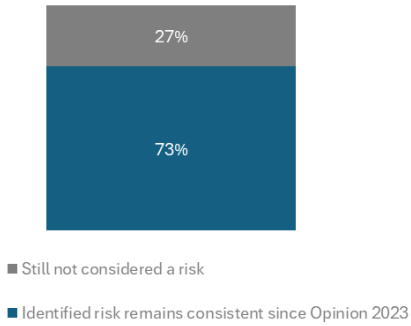
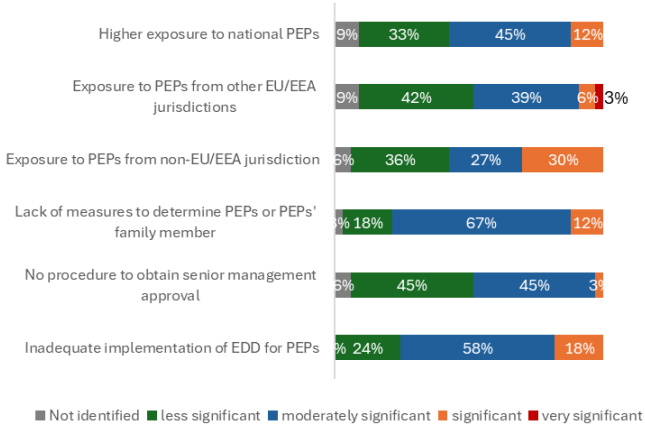


Figure 13: Types of risks identified in relation to PEPs



Box 4. Actions taken by CAs regarding risks associated with PEPs

CAs took various actions to raise awareness of ML/TF risks associated with PEPs and to find ways to mitigate these risks: 35% of CAs updated their guidelines on CDD or published specific guidelines on EDD for PEP. One CA mentioned that their guidelines reference the PEP database, developed and maintained by the State Revenue Service, which is accessible to financial institutions. Three out of 34 CAs updated their sectoral risk assessments with risks associated with PEPs. More than a quarter of CAs organised conferences on corruption or training related to risks associated with PEPs. Several CAs mentioned a systematic analysis approach when specific topics are widely reported in the media, to decide whether they require targeted control and/or communication approaches for financial institutions under their supervision.

At the individual level of supervised entities, CAs use the annual AML/CFT questionnaire to analyse the fluctuation of PEPs compared to the number of customers. They also assess materiality in terms of deposit and loan volumes, life insurance premiums, and the value of payment transactions or e-money issued. Remedial measures may be requested with supervisory actions in case of discrepancies and no mitigating measures applied. Half of the CAs indicated that policies and procedures for PEPs are scrutinised through full-scope inspections. One CA indicated that final inspection reports over the past three years show deficiencies in this specific area in at least 36% of the inspections, which were remediated through a follow-up process.

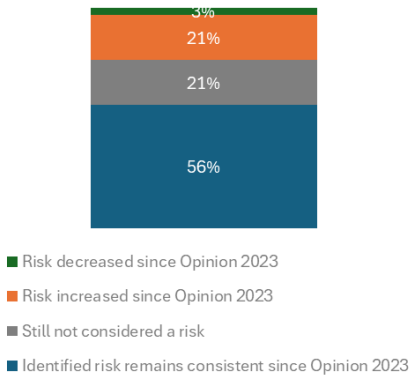
62. **As highlighted in the Europol 2025 SOCTA([20]), corruption affects the financial sector beyond servicing PEPs**. Though laundering the proceeds from corruption remains the main concern, corrupt staff in financial institutions may enable or facilitate money laundering, fuelling organised crime, and pose serious risks to financial stability and security. Individuals with access to digital systems become key targets for corruption as they can provide access to information relevant to the criminal enterprise, while financial institutions may themselves engage in corrupt behaviour, for example to obtain or retain business. Six percent of CAs consider corruption in financial services to be a significant or very significant concern, but the risk is likely to be higher in practice, as corruption in financial services is not exclusively within the remit of AML/CFT supervisors. For example, prudential supervisors or dedicated anti-bribery and corruption (ABC) agencies may also play a role. Further cooperation between ABC authorities and prudential and AML/CFT supervisors would be important.

63. **The Proposal for a Directive on Combating Corruption** (COM/2023/234) introduces **criminal liability for legal persons, including financial institutions, for corruption-related offences.** The directive complements existing AML and Environmental, Social and Governance (ESG) obligations, reinforcing the need for financial institutions to integrate anti-corruption monitoring and mitigating measures into their broader risk management frameworks, thereby addressing certain conduct-related issues.

3.9. Risks of non-compliance with restrictive measures are increasing due to the complexity of successive sanctions measures

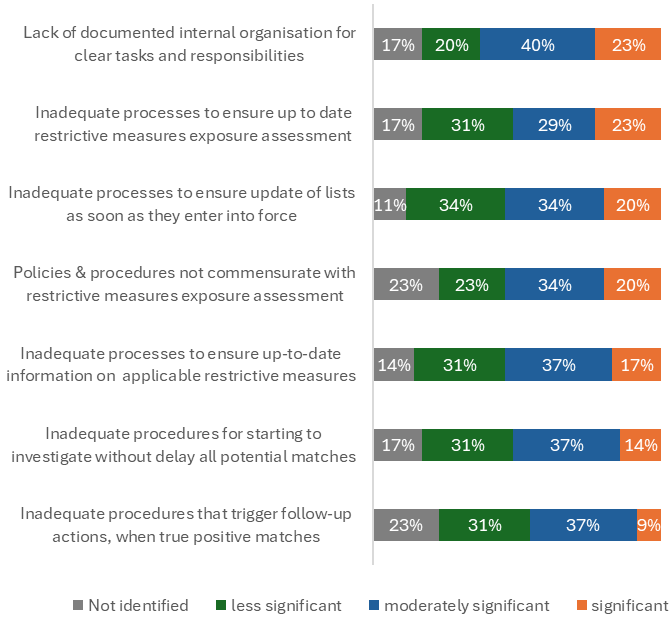
64. **A quarter of CAs consider that the risk of non-compliance with restrictive measures has increased since 2023.** This is due to the number and complexity of EU sanctions measures, which create challenges for financial institutions as sectoral restrictive measures cannot be implemented through standard sanctions screening tools. One CA further noted the operational risk of potential OFAC sanctions related to providing services for OFAC-sanctioned persons not listed by the EU. By contrast, for 21% of CAs, compliance with restrictive measures is not considered a risk.

Figure 14: Evolution of risk compared to risks identified in the 2023 Opinion – Restrictive measures



[20] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

Figure 15: Types of risks identified in relation to controls for implementation of restrictive measures



65. **CAs generally assess institutions' sanctions systems and controls as adequate, though weaknesses persist in some areas.** Risks relate to failure to put in place robust internal processes, governance arrangements, and the adequacy of exposure assessments in particular. Several CAs noted a lack of record-keeping in screening systems, preventing financial institutions from demonstrating that they checked lists before onboarding new customers. There were issues with setting thresholds in screening systems, which prevented effective capture of designated customers. Divergences in the frequency of list updates and screenings were also observed. CAs from Member States that border Russia noted risks of large cash transactions via currency exchanges in connection with the evasion of sanctions imposed on Russia.

66. **Submissions to EuReCA suggest an increase in supervisory action and, consequently, an increase in adverse inspection findings related to restrictive measure systems and controls.** Between 2022 and 2024, 20 CAs submitted 109 material weaknesses to EuReCA. These deficiencies relate to inadequate due diligence concerning customers or their beneficial owner, which prevents proper screening of customers. Internal policies and procedures lacked clear and consistent instructions about responsibilities and tasks for analysing alerts and freezing funds in case of a positive match.

Box 5. Actions taken by CAs to support the implementation of restrictive measures

CAs were asked to explain actions they took to support their supervised sector with the implementation of restrictive measures and targeted financial sanctions. Thirty-six out of 47 CAs indicated they are responsible for assessing the quality of systems and controls for the implementation of restrictive measures and targeted financial sanctions in their sector. Of those responsible authorities, 58% published practical guidance about applicable restrictive measures, the legal framework, including also examples of due diligence, screening best practices, or red flags for circumvention of sanctions. Eleven percent published binding regulations for their supervised sector. Twenty-eight percent of CAs declared that they provided training to their supervised financial sector. Eleven percent set up a dedicated channel to answer questions from the private sector.

Regarding supervisory actions, 30% of CAs carried out off-site supervision, which included specific questions in the annual AML/CFT questionnaire, off-site thematic reviews or reports by external auditors. Half of CAs conducted on-site inspections between 2022 and 2024, either as part of their full-scope AML/CFT inspections or through targeted inspections. Most of these inspections focused on the quality of screening systems, and the effectiveness of policies and procedures to implement restrictive measures.

67. **In November 2024 the EBA published two sets of Guidelines([21]) that, for the first time, set common EU standards on the governance arrangements and the policies, procedures and controls that financial institutions should have in place to be able to comply with Union and national restrictive measures.** The first set of Guidelines is addressed to all institutions within the EBA's supervisory remit. They include provisions that are necessary to ensure that financial institutions' governance and risk management systems are sound and sufficient to address the risk that they might breach or evade restrictive measures. The second set of Guidelines is specific to PSPs and CASPs and specifies what PSPs and CASPs should do to be able to comply with restrictive measures when performing transfers of funds or crypto assets. Both sets apply from 30 December 2025.

Box 6. Challenges related to screening of SEPA instant credit transfers

From the perspective of implementing targeted financial sanctions, Article 5d point (1) of Regulation (EU) 2024/886 states that PSPs have an obligation to screen their client database every calendar day and without delay upon publication of a new list or modification of an existing one, rather than screening transactions (including the payee). This requirement will minimise the risk of making funds available to sanctioned customers. However, PSPs will not be required to take measures to satisfy themselves that the payee PSP's restrictive measures systems and controls are adequate. This might also expose PSPs to a significant risk of breaches of restrictive measures that are not targeted financial sanctions, such as sectoral restrictive measures.

68. **The specific infrastructure of card payment schemes can lead to sanctions breaches.** There is fragmentation in the payment chain, which involves multiple parties such as customers, merchants, acquirers, card issuers, card scheme licensors, and sometimes even subcontractors or third-party acquirers. The card acquirer, as the obliged entity, has access solely to card numbers and payment amounts, without the ability to identify customers by name. This results from a specific exemption under the travel rule of the Funds Transfer Regulation([22]) (FTR), which applies exclusively to card-based acquiring services and should not be interpreted as extending to all acquiring services. The authorisation message received by the card issuer (e.g. a credit institution) often contains only an identifier, such as the trading location, which can be easily altered. Furthermore, while card payment schemes screen their partners (issuers and acquirers), they do not screen cardholders or merchants. A similar risk exists with issuing banks: a non-EU bank could issue a card to a sanctioned individual, who could then use it via an EU acquirer. Typically, only limited screening is conducted on card transaction data.

69. Payment cards that aggregate multiple debit/credit cards into a single payment instrument ('aggregator' cards or 'meta cards') pose emerging ML risks and may facilitate evasion of targeted financial sanctions. They obscure the source or use of funds, as merchants and acquirers see only

[21] EBA/GL/2024/14 and EBA/GL/2024/15.

[22] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto assets and amending Directive (EU) 2015/849.

the PSP providing the aggregator card as their counterparty (i.e. the link between the end user's spending and the underlying funding instrument is not transparent). This may be exacerbated as users can link cards issued in various countries and retroactively change which funding card paid for a transaction ('go back in time' features).

70. Inconsistent implementation of targeted financial sanctions will be reduced under the new AML/CFT framework. Under the AMLR, risks of non-implementation and evasion of targeted financial sanctions will be part of the Union-wide risk assessment, national risk assessments and business-wide risk assessment by financial institutions. AML/CFT supervisors, and AMLA in its supervisory role, will have a monitoring role to ensure compliance by obliged entities with regard to their obligations in relation to targeted financial sanctions.

3.10. Automation and AI drive the rapid expansion of sophisticated fraud and cybercrime schemes

71. **The 2024/2025 EBA Consumer Trends Report([23]) identifies payment fraud as the most significant issue for EU consumers**. Furthermore, according to the Europol 2025 SOCTA([24]), fraud schemes constitute the most rapidly expanding sector in organised crime, targeting a broad spectrum of victims, including individuals, public and private sector organisations and their data, and generating large profits. The June 2025 EBA Risk Assessment Report([25]) highlights that fraud risk has grown sharply in the last two years, from 33% agreement in the March 2023 RAQ to 52% in March 2025, and is now considered the second most relevant operational risk, according to the Risk assessment questionnaire to banks.

72. **The scale, diversity and sophistication of fraudulent activities are previously unseen, driven by advancements in automation and AI.** These schemes leverage AI to create highly realistic narratives that incorporate trending societal topics, making them increasingly convincing. Fraudsters are also adapting their techniques to elude the application of the strong customer authentication requirements imposed by EU law.

Box 7. Case study on misuse of AI during remote onboarding

In a review conducted in 2024 by a CA, several financial institutions identified remote onboarding as a risk factor that increases their exposure to being used for laundering the proceeds of scams or fraud. Multiple cases illustrate how criminal networks are exploiting new generative artificial intelligence technologies – such as deepfakes – to bypass standard remote identity verification measures. The intensity of efforts by criminal organisations to open or use payment accounts for laundering the proceeds of scams or fraud is assessed as very high. These efforts include impersonating real individuals, using false identities, purchasing existing companies, or relying on 'money mules' – legitimate customers who lend or transfer control of their accounts for the purpose of laundering illicit funds.

73. **Credit institutions, investment firms and investment fund managers are particularly vulnerable.**

[23] EBA/REP/2025/08.

[24] European Union Serious and Organised Crime Threat Assessment 2025.

[25] EBA Risk Assessment Report June 2025.

- Thirty-six percent of CAs supervising credit institutions consider the risk of fraud to be significant or very significant. For example, in one Member State, the number of STRs related to fraud has increased by more than 35% since 2021. There is a rise in cybercrime using advanced fraud techniques such as phishing, malware and ransomware to gain access to bank accounts and facilitate money laundering operations.

- In the CIU/fund managers and investment firms sectors, most CAs identified inherent risks stemming from various types of investment fraud, including Ponzi schemes, pyramid schemes and 'boiler-rooms'. In these schemes, services for investment operations are provided by individuals or companies not authorised to operate in the securities markets, targeting victims recruited by phone or web portals. Cryptocurrency holds a central role, both as a payment method and as a vehicle for investment fraud. Investment fraud and business email compromise remain the most prolific online fraud schemes.

74. **The use of AI for money laundering can automate financial schemes and leverage deep-fake technologies to evade AML/FT measures like identity control**. In the credit providers sector, CAs observed a high level of use of falsified ID cards to open new payment accounts and acquire credit, especially with online platforms. Some CAs of EMIs and PIs observed a shift of money mulers from the traditional banking sector to other means of money transfers.

75. **In 2024, the EBA and ECB issued a Joint Report on payment fraud in the EU([26])**. This is the first publication of such comprehensiveness in the EU and will be updated annually. The key messages from this first edition are that the introduction of strong customer authentication has been successful in reducing fraud in the EU, but that fraudsters have created new attack vectors. As a result, there was EUR 4.3 bn in payment fraud in 2022, and another EUR 2.0 bn in the first half of 2023.

76. **In 2024, the EBA also issued an Opinion on new types of payment fraud and possible mitigants([27])**. This Opinion is addressed to the EU legislators and sets out recommendations for how these new types of fraud could be mitigated through the revision of PSD2 and the creation of PSD3.

3.11. Information gaps in payment schemes' infrastructure complicates compliance with AML/CFT obligations

77. **CAs point to risks associated with ATM withdrawals when cardholders are not clients of the financial institution operating the ATM**. These cards may be linked to deposit, payment or electronic money accounts held in other Member States or third countries, exposing such transactions to cross-border money laundering risks. In the absence of data identifying the cardholder, the institution operating the ATM must be able to detect unusual patterns of cash withdrawals – using, for example, the date, time and location of the transaction, and the amount and breakdown of the requested sum.

[26] 2024 Report on payment fraud.

[27] EBA/Op/2024/01.

78. Until now, certain types of ATM operators have been excluded from the scope of PSD2. Specifically, ATM operators that only offer cash withdrawals and are not party to a framework contract with the cardholder are exempt from PSD2, provided they act on behalf of the card issuer. As a result, they are not considered PSPs under PSD2 and may also fall outside the scope of AML obligations. However, the proposed Directive on Payment and Electronic Money Services – which will effectively become PSD3 – explicitly addresses this exemption.

Box 8. Challenges related to transaction monitoring of SEPA instant credit transfers

Many CAs noted that instant payments, executed in 10 seconds, 24 hours a day and 7 days a week, present challenges for effective transaction monitoring. AML/CTF and fraud prevention techniques may be hindered. The 10-second rule impedes checks to stop unusual transactions between initiation and execution, making it difficult to recognise fraud scenarios early. As a result, transactions may be carried out, potentially facilitating money laundering. In addition, effective adverse media checks and other observations are part of AML/CTF and fraud prevention systems. These may suffer under the 10-second rule, reducing their effectiveness.

Guideline 4.74 of the EBA Risk Factors Guidelines is relevant. It states that financial institutions should define the transactions they monitor in real time and those they monitor after completion, in line with their risk level, as well as the risk factors (combined or not) that should trigger *ex ante* monitoring. For instance, transactions ceilings for self-service online banking may in part mitigate such risks: transactions that do not fit with the customer profile are subject to prior validation by the staff of the PSP.

The revision of the PSD will also be an opportunity to stress the importance of effective *ex ante* monitoring.

3.12. Competent authorities took actions to tackle de-risking practices

79. **De-risking occurs if a financial institution decides not to provide a financial service to a customer.** It can be a necessary risk management tool. But de-risking can also be unwarranted, for example if an institution does not take into account an individual customer's risk profile.

80. **The 2024/2025 EBA Consumer Trends Report (CTR)([28]) suggests that 'de-risking' remains an important issue for EU consumers.** The CTR summarises the views of national consumer protection authorities, consumer associations, industry associations and national ombudsmen, among others. The information received for the CTR does not distinguish between warranted and unwarranted de-risking.

81. **By contrast, 40% of CAs indicate that unwarranted de-risking has decreased.** Another 40% suggest that de-risking is not an issue in their Member State. This assessment is backed up by the small number of material weaknesses linked to de-risking in EuReCA (10 material weaknesses between 2022 and 2024).

[28] EBA/REP/2025/08.

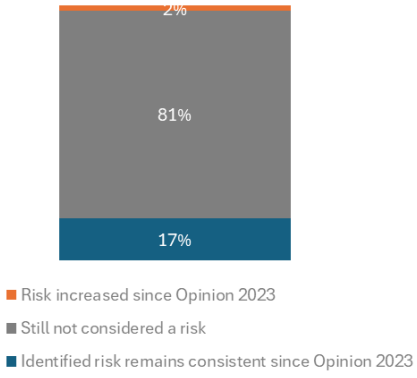
82. **80 % of CAs took action to tackle unwarranted de-risking following the publication of EBA Guidelines on tackling de-risking([29])([30]).** This included the implementation of the EBA Guidelines, outreach activities such as circular letters and briefings, and regular meetings with affected stakeholders. Half of all CAs took steps to assess their sector's compliance with the EBA Guidelines, as part of their on-site or off-site inspections or as part of thematic reviews.

83. **The EBA is now assessing possible next steps because access to basic financial products and services is an important public interest goal.** These next steps are likely to include joint guidelines for which the EBA and AMLA have a mandate under Article 21(4) of the AMLR.

3.13. Risks related to laundering proceeds from environmental crimes are rarely identified, but some competent authorities are taking action due to the prevalence of waste trafficking

84. **A growing number of Member States assess ML/TF risks associated with environmental crime but two thirds of all Member States have not yet assessed this risk.** Eighty-one percent of CAs therefore do not consider the laundering of proceeds from environmental crimes as a risk.

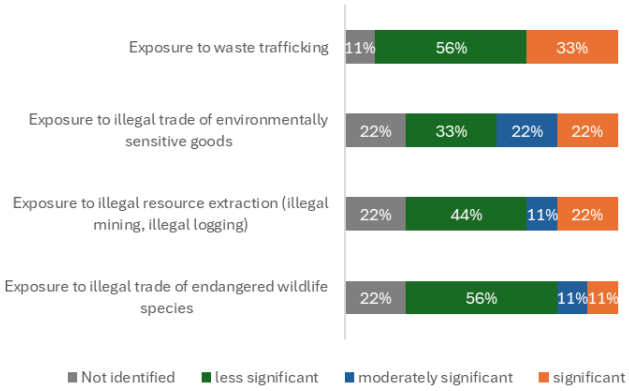
Figure 16: Evolution of risk compared to the risks identified in the 2023 Opinion – Laundering of proceeds from environmental crimes



[29] Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services – EBA/GL/2023/04.

[30] Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849 – EBA/GL/2023/03

Figure 17: Types of risks identified in relation to environmental crimes



85. **In spite of this, 33% of CAs consider that waste trafficking poses a significant risk**. This is in line with the 2025 Europol SOCTA, which points to a growing number of violations related to waste trafficking procedures and pollution crimes. Waste trafficking is increasingly committed from within the waste management sector, blurring the lines between licit and illicit operations. Some CAs have therefore instructed their sectors to closely monitor customers in the waste management industries. They have also highlighted instances of corruption involving public decision-makers, especially in the management of hazardous waste.

86. **22% of CAs consider that the risk of exposure to illegal resource extraction and illegal trade of environmentally sensitive goods is significant.** Wood logging and processing, in particular, appear to stand out. By contrast, according to CAs, ML/TF the proceeds from illegal trade of endangered wildlife species does not appear to be a particular concern for financial institutions in the EU.

Box 9. Actions taken by CAs in relation to environmental crimes

In response to the 2023 Opinion, CAs were encouraged to assess the risk that their supervised entities might be involved in laundering proceeds from environmental crimes. Fifty-two percent of CAs (25 in total) did not take any direct action. Some CAs did not engage in supervisory activities but trained their staff to recognise the risks associated with laundering proceeds from environmental crimes.

Many CAs reported monitoring emerging typologies, often in collaboration with environmental crime authorities, and incorporating these risks into their broader risk assessments. A few CAs took more proactive steps: five issued guidance through roundtables or publications, four added relevant questions to their annual AML/CFT questionnaires, and others began evaluating how well financial institutions classify high-risk customers in sectors linked to environmental crime.

87. **In January 2025 the EBA published guidelines on the management of ESG risks([31])**. The guidelines specify the content of plans to be prepared by institutions with a view to monitoring and addressing the financial risks stemming from ESG factors.

[31] EBA/GL/2025/01.

4. AML/CFT trends by sector

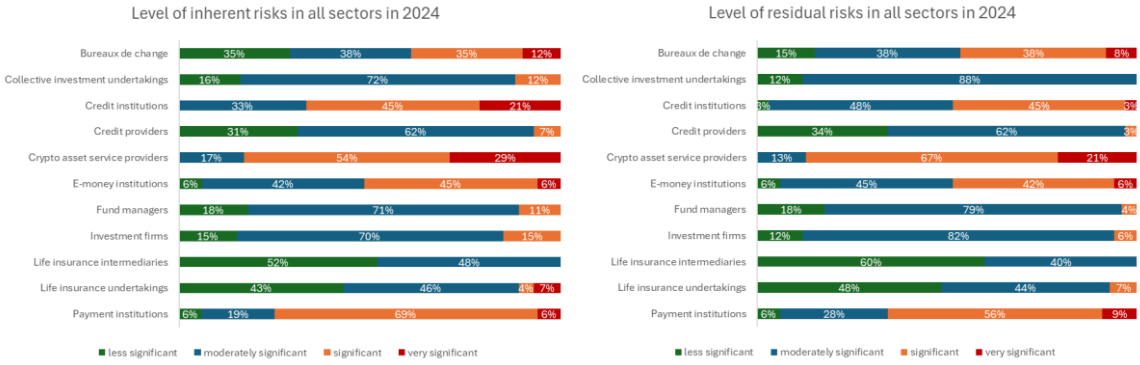
88. This section provides an overview of the main findings on risk levels in each of the sectors under the EBA's remit. More granular information, including detailed graphs by sector, is available in Annex I.

4.1. AML/CFT controls are becoming more effective in some sectors

89. **Since 2021, the levels of inherent risk have remained broadly stable across most sectors([32]).** Inherent risks have increased in the payment and e-money institutions, crypto asset service providers and life insurance undertakings, which are an exception to this trend (Figures 24, 26, 28 and 34).

90. **At the same time, controls are increasingly put in place and are being assessed as adequate more often than was previously the case.** As a result, residual risk levels are improving, with marked reductions in the overall levels of residual risk in the credit institutions, investment funds and life insurance sectors in particular (Figures 44, 52 and 51). By contrast, controls appear to be less effective in the e-money and credit provider sectors, as no marked reduction in risk levels was observed (see Figures 46 and 48). In three sectors, payment institutions, bureaux de change and CASPs, information provided by CAs suggests that levels of residual risk exceed inherent risks (see Figure 18). This could be due to CAs assessing the adequacy and effectiveness of AML/CFT systems and controls as poor overall.

Figure 18: Overview of inherent ML/TF risks and overall ML/TF risk profile in all sectors in 2024



91. **Between 2021 and 2024, levels of inherent risks have decreased in six sectors:**

— **Credit institutions:** 66% of CAs consider that the sector is exposed to significant or very significant levels of inherent ML/TF risk, down from 73% in 2021. CAs suggest that this is due to a reduction in inherent risks linked to products/services and delivery channels (Figures 22 and 23).

— **Credit providers**: CAs now consider the level of inherent risk in the sector to be moderately significant or less significant across all categories (Figures 30 and 31).

[32] See more details in Section 1 of Annex I.

- **Investment firms**: Most CAs assess all risk categories as moderately significant, with two CAs downgrading their risk assessment from very significant in 2021 to significant in 2024. One CA nevertheless reported a 220% increase in authorisations of investment firms and classified their products/services as posing a very significant inherent risk (Figures 38 and 39).

- **Collective investment undertakings**: Most CAs assess the sector as presenting a moderate risk. The reduction in overall inherent risk levels is due to a reduction in risk levels for customers, geography and delivery channels. One CA noted that significant risks remained in relation to real estate trading (Figures 40 and 41).

- **Fund managers**: The sector is considered by most CAs as presenting a predominantly moderate and less significant risk from a ML/TF perspective. Inherent risks in products and geography remain stable, while the risk level of customers and delivery channels decreased compared to 2021. Nevertheless, new risks appear to emerge: two CAs observed a higher proportion of third country (non-EU) and high-risk country investors in investment funds managed by registered asset management companies compared to authorised asset management companies and investment firms. Registered asset management companies also usually invest in higher-risk assets (e.g. private equity, real estate, real assets, infrastructure, crypto). This increases the risk exposure of these registered asset management companies, which have to start managing one or several investment funds before being registered (Figures 42 and 43).

- **Life insurance intermediaries (LII)**: Half of all CAs now consider the LII sector's exposure to ML/TF risks to be less significant, while almost another half consider the sector to be moderately significant. Categories of risks related to products/services, delivery channels and geographies remain stable, while the share of significant risks related to customers has decreased. CAs reported risks associated with complex life insurance policies being exploited to launder illicit funds (Figures 36 and 37).

92. **The level of inherent risks remains stable for bureaux de change, though the share of very significant risks linked to by-products and geographies has increased** (Figures 32 and 33). This is due to the provision of high-risk services such as brokering gold and precious stones and the conversion of cash via chargebacks. Hawala transfers can be related to criminal activities and have evolved with new delivery channels. One CA reported an increase in risks associated with hybrid hawala banking, which is conducted using digital channels such as smartphone apps.

93. **The level of inherent risks has increased in the payment and e-money institutions, life insurance undertakings and CASP sectors:**

- **Payment institutions:** Almost 70% of CAs assess the overall level of inherent risk of payment institutions as significant, which represents an increase from the 59% in 2021. Though this is high, the proportion of 'very significant' inherent risk has halved between 2021 and 2024, due to a perceived reduction in ML/TF risks associated with customers, products and services (Figures 24 and 25).

- **Life insurance undertakings (LIU)**: The LIU sector is considered as presenting a moderately significant or less significant risk from an inherent ML/TF perspective by most CAs. Compared to the previous Opinion, three CAs have increased their inherent risk ratings due to the very significant risk they associate with some of the sector's products and services

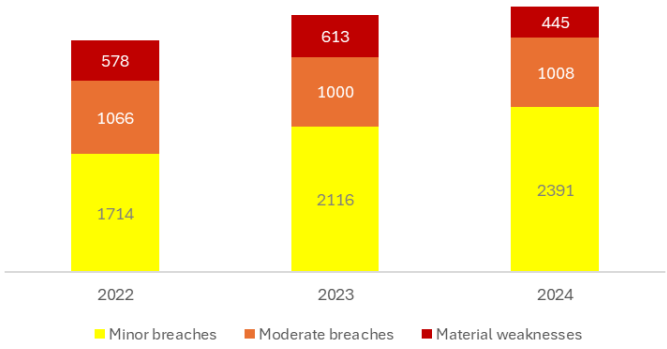
(Figures 34 and 35). This risk is related to unit-linked products possibly used to introduce illicit money into the financial system, as the beneficiaries can switch.

— **E-money institutions**: An increasing number of CAs assess the inherent risk associated with the sector as significant to very significant (Figures 26 and 27). CAs point to the use of electronic money services to collect funds on social platforms for TF. The growing provision of EMTs is also of concern.

— **Crypto asset service providers**: More than half of all CAs consider CASPs to present a significant risk, with products and services and delivery channels representing the largest proportion of very significant risks. This applies in particular to the conversion of crypto and fiat currencies (and vice versa), and to self-hosted wallets. More than half of CAs consider customers to pose significant inherent risk for CASPs, while geography remains a moderately significant risk (Figures 28 and 29).

4.2. Most AML/CFT breaches relate to CDD measures

Figure 19: Evolution of total breaches in all sectors



94. **There has been a consistent increase in minor breaches over the past five years**. The number of minor breaches more than doubled from 2020 to 2024 and increased by 40% between 2022 and 2024, the period covered by the 2025 Opinion. The increase in the number of breaches may be due to the 40% increase in off-site reviews conducted between 2022 and 2024, rather than worsening AML/CFT controls.

95. **The number of moderate breaches remains broadly stable, while numbers of serious breaches fluctuate**. Figures from 2022 to 2024 encompass material weaknesses submitted to EuReCA, covering ineffective or inappropriate application, potential breaches and breaches. There was a notable decrease in 2024, bringing the number down to 445 breaches. This might be related to a delay in the reporting by CAs to EuReCA.

96. **Most breaches relate to CDD measures, across all sectors.** However, the nature of the breaches varies by sector.

— As was the case in previous years, credit institutions tend to have CDD policies and procedures in place but fail to apply them effectively. Failures in customer risk ratings were also frequently reported.

— Deficiencies in effectiveness of ongoing monitoring were identified in credit institutions, e-money institutions, bureaux de change, CIU/fund managers, and investment firms. This suggests that many financial institutions still struggle to put in place risk assessment models that correctly reflect the ML/TF risk of their own customers and to adjust their risk mitigation efforts in line with that risk. A large number of deficiencies are also linked to an improper calibration of transaction monitoring and screening systems.

— Failures in customer identification were reported in e-money institutions, bureaux de change, and credit providers, while weaknesses in customer verification were more prevalent in credit institutions and payment institutions. LIUs had failures in the identification of PEPs.

Case study 1 from EuReCA

Breaches in relation to customer identification, monitoring of business relationships and transactions, internal control systems and compliance with international sanctions were found at an EMI, which subsequently faced a withdrawal of authorisation in 2024.

97. **Failures in wider AML/CFT systems and controls are the second most common issue**. Institutions across six sectors are particularly affected: credit institutions, payment institutions, e-money institutions, credit providers, bureaux de change and LIUs. According to CAs, bureaux de change and payment institutions were most likely to fail to put in place adequate internal policies and procedures. Weaknesses in the effective application of internal policies and procedures were identified across all six sectors, as well as in crypto asset service providers, which also lacked adequate AML/CFT human and material resources.

Case study 2 from EuReCA

One payment institution had serious breaches and shortcomings in AML/CFT structures, processes and controls, leading to critical issues in transaction monitoring, reporting of suspicious transactions and data retention. The CA imposed a prohibition on opening new accounts and required remedial measures, while the sanctioning procedure is ongoing.

98. **Deficiencies in risk management are common in five sectors**. A lack of a business-wide risk assessment was prevalent among credit providers. For other sectors – namely CIU/fund managers, LIIs and crypto asset service providers – deficiencies related to the adequacy of the business risk assessment were common.

Case study 3 from EuReCA

One CASP had deficiencies in its methodology for assessing business-wide and customer-related ML/TF risks, leading to inadequate evaluations of customer business and risk profiles. In 2024, the CASP was issued an administrative penalty of EUR 440 000 along with several orders to comply.

99. **Failures in the reporting of suspicious transaction affect investment firms in particular, followed by credit institutions, e-money institutions and payment institutions.** Deficiencies in

the existence and adequacy of STR-related policies and procedures were frequently observed in CIU/fund managers and LIIs.

> **Case study 4 from EuReCA**
>
> Serious CDD deficiencies, transaction monitoring deficiencies and delays in reporting STRs were identified in a neobank in 2024. The CA imposed a EUR 9.2 million fine and several administrative measures in 2024.

100. The **overall residual risk profile improved between 2021 and 2024 in eight sectors**: credit institutions, credit providers, e-money institutions, bureaux de change, LIIs (Figures 44, 48, 46, 49 and 51), and the three sectors of financial markets: investment firms, collective investment undertakings and fund managers (Figures 52, 53 and 54). This suggests that AML/CFT controls have improved over the period in these sectors.

101. If the percentage of very significant residual risk in **e-money institutions** remains stable at 6%, the **percentage of less significant residual risk improved from 3% to 6% and the share of significant residual risks decreased slightly from 44% to 42%** (Figure 46).

102. Regarding **bureaux de change, there was a shift from very significant residual risk** (from 14% in 2021 to 8% in 2024) **to significant residual risk** (from 32% in 2021 to 38% in 2024), while the ratio of less significant and moderately significant residual risks has remained stable (Figure 49). However, this is one of the three sectors with payment institutions and CASPs where significant and very significant levels of residual risks are higher than the levels of inherent risks, which indicates deficiencies in AML/CFT controls.

103. The **overall residual risk profile increased in three sectors: payment institutions, LIUs and crypto asset service providers** (Figures 45, 50 and 47). While the percentage of very significant residual risks remains stable at 9% for payment institutions, the number of less significant residual risks went down from 16% in 2021 to 6% in 2024, and the number of significant risks increased slightly from 53% in 2021 to 56% in 2024. However, CAs remain concerned that the poor quality of controls – particularly among newly authorised entities – is insufficient to mitigate the high inherent risk levels and may create vulnerabilities that could increase inherent risk levels in the medium to long run. CAs of LIUs assessed the residual risks of the sector with an increase from moderately significant to significant, and a shift of 4% between the two categories. CAs noted an increasing use of 'InsurTech' based on remote transactions only, with inadequate CDD and intermediaries not fully aware of AML/CFT regulations. For CASPs, the percentage of very significant residual risks increased from 19% in 2021 to 21% in 2024, while significant residual risk went up from 52% to 67%. This may be due to the 2.5-fold rise in authorisations of CASPs between 2021 and 2024 and the lack of maturity of AML/CFT compliance among newcomers to the sector, as indicated by the overall level of residual risks exceeding the level of inherent risks (Figure 18).

4.3. Focus on trends in supervision

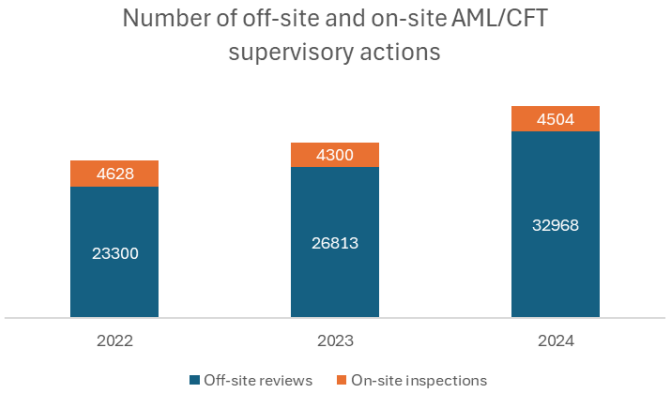
4.3.1. Trends in supervision from 2022 to 2024

104. **There is a significant and consistent increase in the number of off-site reviews over the three-year period**. The number of reviews increased by 41% from 2022 to 2024. This suggests a

growing emphasis on remote supervisory activities, possibly due to advancements in technology and a shift towards more risk-based and targeted supervisory methods.

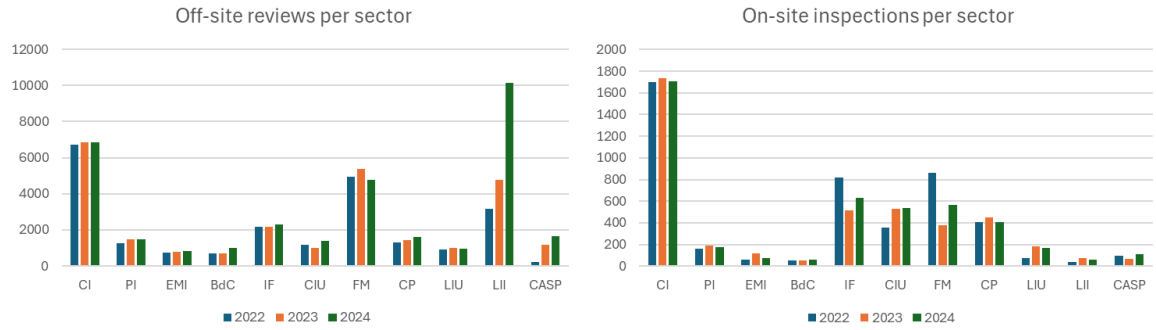
105. **The number of on-site inspections shows a slight decrease from 2022 to 2023, followed by a small increase in 2024.** Overall, the number of on-site inspections remains relatively stable, with minor fluctuations. This indicates that while off-site reviews are increasing, on-site inspections continue to play a crucial role in supervisory actions for higher-risk sectors or activities.

Figure 20: Total number of off-site and on-site AML/CFT supervisory actions



106. **The number of supervisory activities cannot be directly compared across sectors, as each sector varies in size and risk profile.** In line with a risk-based supervision approach, fewer supervisory activities are expected in lower-risk sectors or in sectors that are very small.

Figure 21: Off-site reviews and on-site inspections per sector



Off-site reviews

107. Off-site reviews of credit institutions, investment firms and LIUs show stability, with minor increases over the period (2%, 6% and 4% respectively).

108. The number of off-site reviews for payment institutions, e-money institutions, credit providers and bureaux de change exhibit consistent growth (PI: 18%, EMI: 9%, CP: 23%, BdC: 41%). Theis 40% spike in off-site reviews of bureaux de change is due to scheduled off-site reviews carried out by one CA, targeting its obliged entities with very significant, significant and moderately significant risk profiles. Previously, in 2022 and 2023, 80% of off-site reviews were

conducted by the two CAs, with the two largest numbers of bureaux de change with very significant risk profiles (one in the eurozone, one outside).

109. Off-site reviews of crypto asset service providers have seen significant increases, by +431% between 2022 and 2023, followed by a 39% increase in 2024, indicating heightened regulatory focus, due to the 2.5-fold increase in authorisations of CASPs between 2021 and 2024 and the transposition of AMLD5 into national laws.

110. The number of off-site reviews of fund managers and collective investment undertakings show fluctuations, with notable increases and decreases. There was a decrease in reviews for collective investment undertakings in 2023 (-16%), followed by a significant increase in 2024 (+38%), resulting in a 16% increase between 2022 and 2024. Reviews for fund managers increased in 2023 (+9%) but decreased in 2024 (-11%), showing a -3% fluctuation between 2022 and 2024.

111. The spike of 112% in off-site reviews of LIIs between 2023 and 2024 was due to the number of periodic AML/CFT returns requested by one CA from all its supervised LIIs.

On-site inspections

112. Notable increases in on-site inspections are seen in sectors like LIUs and e-money institutions, while sectors like fund managers and investment firms show significant fluctuations.

113. The credit institutions and credit providers sectors have shown stability in the number of on-site inspections received. There was a minor increase in 2023 (credit institutions +2% and credit providers +11%), followed by a return to the same amount in 2024.

114. On-site supervision increased by 22% for bureaux de change, 27% for e-money institutions, and 8% for payment institutions.

115. The number of on-site supervisory actions rose by 122% for LIUs and by 53% for LIIs.

116. On-site supervision of crypto asset service providers decreased by 34% between 2022 and 2023 but increased overall by 14% between 2022 and 2024, correlated with the 2.5-fold increase in authorisations of CASPs between 2021 and 2024.

117. Investment firms and fund managers have shown a gradual decrease in on-site supervision, at -23% for investment firms and -34% for fund managers. During the same period, collective investment undertakings have shown a gradual and significant increase, with a 52% rise. The rise for CIUs can be correlated with the decrease in on-site inspections of fund managers, as there was a shift in scope in five MS.

4.3.2. Summary of measures undertaken by the competent authorities pursuant to the proposals set forth in the 2023 Opinion

118. In the 2023 Opinion, the EBA issued proposals to the CAs to address risks identified in various sectors. Below is a summary of actions taken by the CAs in response to these recommendations.

119. **Risk assessment and risk-based supervision: CAs were asked to take actions to ensure sufficiently risk-based and intrusive supervision, to adjust their supervisory plans** according to the ML/TF risk profile of individual institutions, and to the ML/TF risks in that sector.

- Many CAs across sectors (e.g. credit institutions, EMIs, CIUs) revised or enhanced their risk assessment methodologies and tools, incorporating new indicators such as cross-border activity, virtual IBANs, or sector-specific risks.
- Many CAs also conducted or updated their sectoral risk assessment in sectors such as credit providers, bureaux de change and LIUs to better understand emerging risks.
- AML/CFT questionnaires have been widely used for data collection on risks across sectors and for off-site supervision.

120. **Intrusive on-site inspections and off-site reviews: CAs were asked to test the effectiveness of key AML/CFT controls and address identified weaknesses.**

- Targeted and thematic inspections were common across all sectors, focusing on high-risk areas such as transaction monitoring, onboarding procedures and agent oversight.
- CAs used intrusive off-site reviews to complement or precede on-site inspections, especially in sectors such as fund managers and e-money institutions.
- CAs tested IT systems during on-site inspections and also assessed the effectiveness of IT systems with virtual walkthroughs. Some CAs developed in-house tools for risk-based sampling and data analysis (e.g. for credit institutions). The use of blockchain analytics and AI was noted in crypto and payment sectors to assess transaction risks.
- Some CAs engaged external consultancy support to enhance supervisory strategies (e.g. for payment institutions and e-money institutions).

121. **Guidance and communication:** CAs of three sectors (payment institutions, e-money institutions and investment firms) were **asked how they provided specific guidance to the sector to ensure that supervisory expectations** regarding adequate and effective AML/CFT systems and controls **are well understood and applied**.

- Many CAs issued updated guidelines and handbooks to clarify supervisory expectations and address identified weaknesses.
- CAs organised training and awareness sessions across sectors to share findings, typologies and best practices.
- CAs also used individual feedback and post-inspection letters as tools for guidance.

122. **Further details on sector-specific measures** – such as the enhanced supervision of agent networks in the payment institutions sector, the identification of key risks in each subsector of credit providers, and the oversight of outsourced functions by investment firms and fund managers – are **provided in Annex II**.

Annex I: Graphs by sector

1. Level of inherent risks

Credit institutions

Thirty-two CAs responsible for the AML/CFT supervision of 4 865 credit institutions (CI) responded to the EBA's questionnaire.

Figure 22: Inherent ML/TF risks in the credit institutions sector

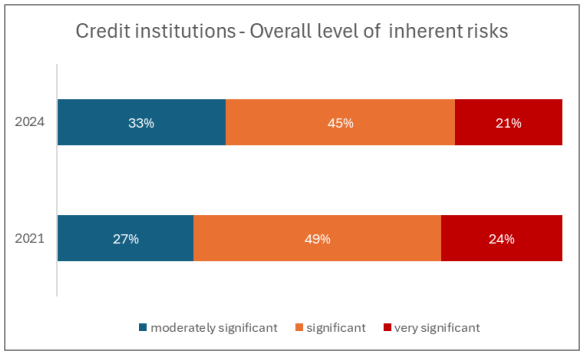
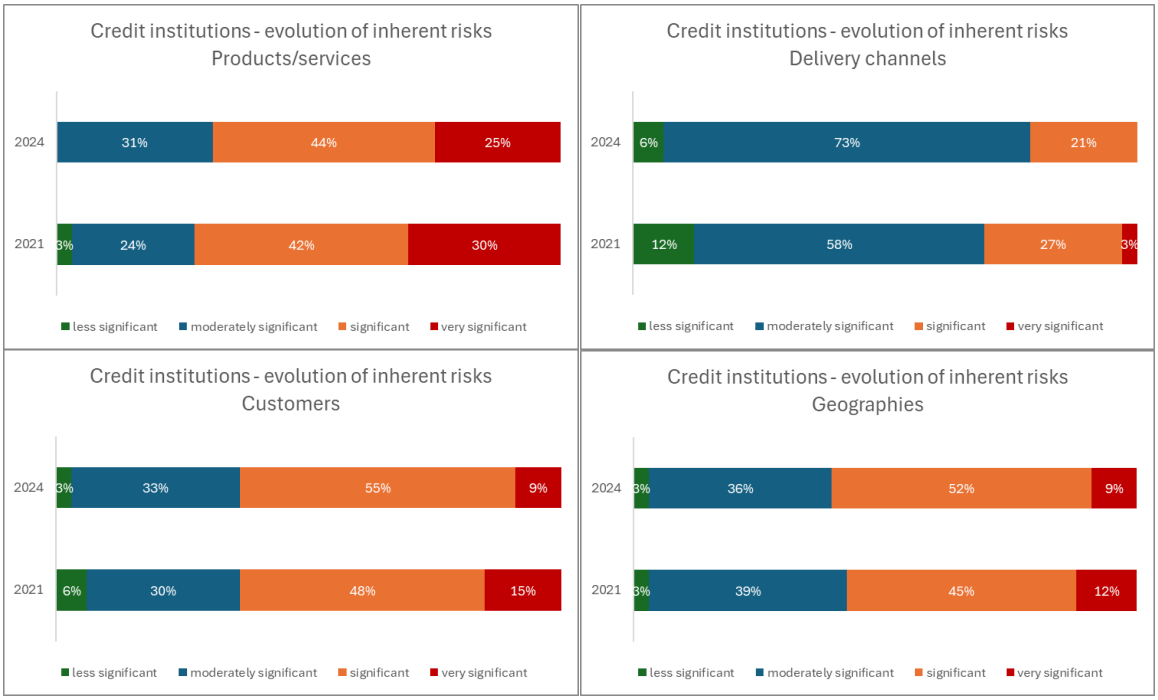


Figure 23: Factors of inherent ML/TF risks in the credit institutions sector



Payment institutions

In total, 31 CAs, responsible for the AML/CFT supervision of 6 556 obliged entities in the payment institutions (PIs) sector, responded to the EBA's questionnaire for 2024.

Figure 24: Inherent ML/TF risks in the payment institutions sector

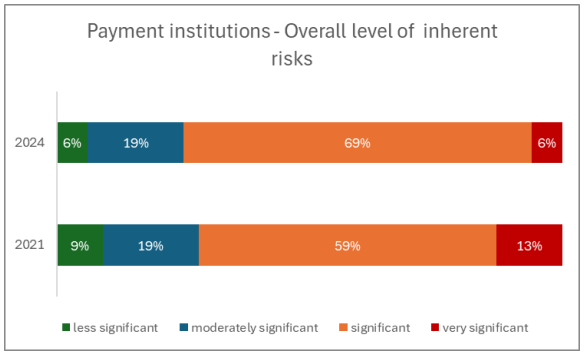


Figure 25: Factors of inherent ML/TF risks in the payment institutions sector

E-money institutions

In total, 31 CAs responsible for the supervision of 729 EMIs responded to the EBA's questionnaire. The 70% increase in EMI between 2021 and 2024 stems from a large increase in one MS, where agents of EMI are now counted as separate obliged entities. In 2021, the sector was highly concentrated in 2021, with more than half of all EMIs based in six Member States. Since then, the sector has undergone a significant shift, with all Member States except for five experiencing large increases in authorisations or withdrawals of EMI licences.

Figure 26: Inherent ML/TF risks in the e-money institutions sector

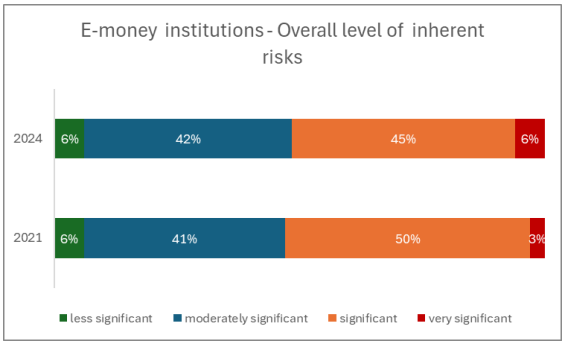


Figure 27: Factors of inherent ML/TF risks in the e-money institutions sector

Crypto asset service providers

In total, 23 CAs, responsible for the AML/CFT supervision of 2 525 obliged entities that are CASPs, responded to the EBA's questionnaire in respect of data for 2024. CAs in four new MS compared to 2021 are now supervising CASPs.

Figure 28: Inherent ML/TF risks in the crypto asset service providers sector

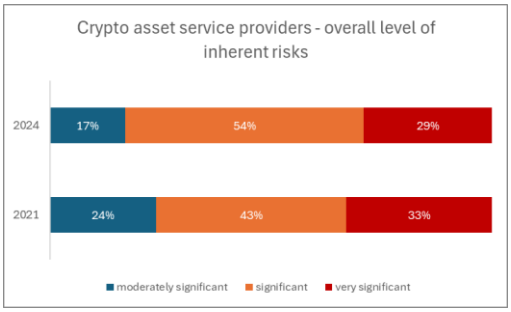
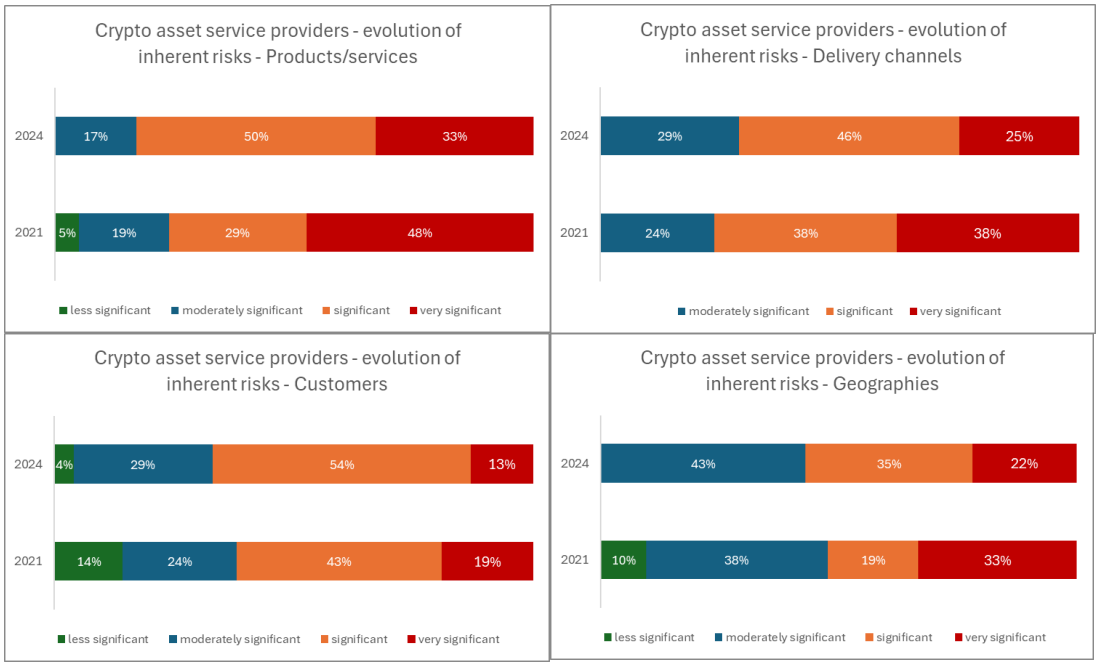


Figure 29: Factors of inherent ML/TF risks in the crypto asset service providers sector



Credit providers

The EBA received responses from 26 CAs responsible for the AML/CFT supervision of a total of 2 212 credit providers (CPs) for 2024.

Figure 30: Inherent ML/TF risks in the credit providers sector

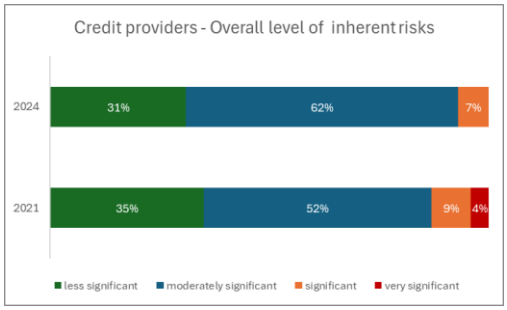
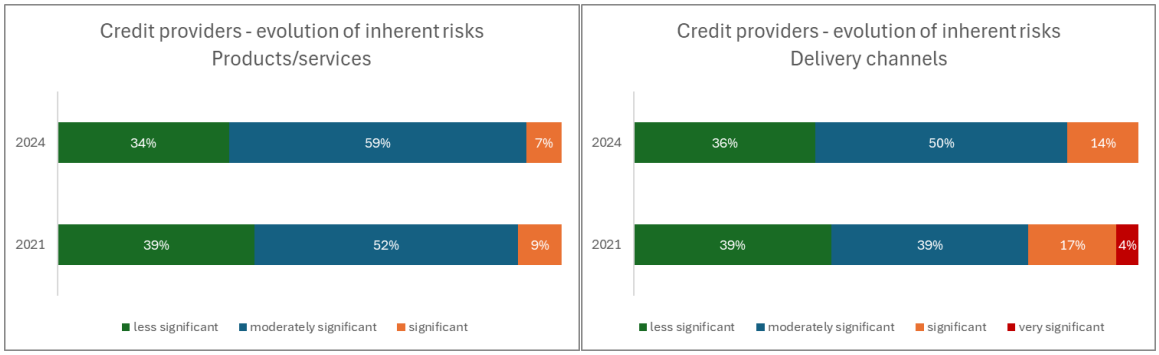
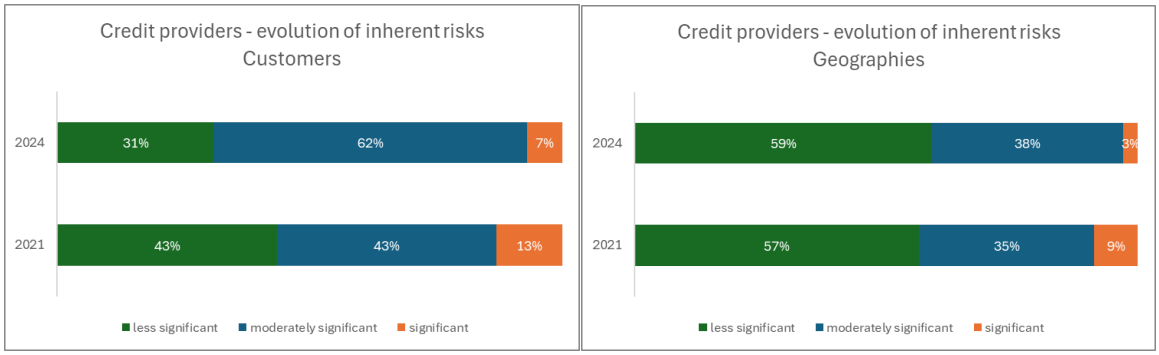


Figure 31: Factors of inherent ML/TF risks in the credit providers sector





Bureaux de change

Twenty-six CAs responsible for the AML/CFT supervision of 4 545 firms providing currency exchange services (bureaux de change – BdC) responded to the EBA's questionnaire in respect of 2024. The BdC sector is concentrated in Member States outside of the Eurozone, with 81% of the BdC based there. The remit of CAs that provided data for 2024 and for 2021 in the previous Opinion has changed: Five additional CAs submitted data for 2024 but did not do so in 2021, while two CAs that provided data for 2021 did not respond with data for 2024.

Figure 32: Inherent ML/TF risks in the bureaux de change sector

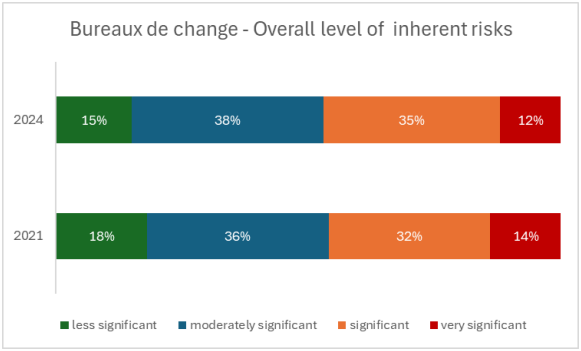
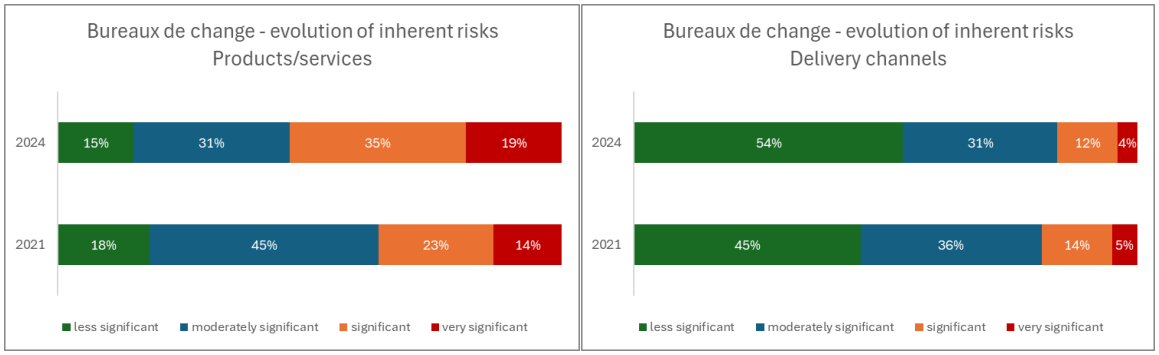
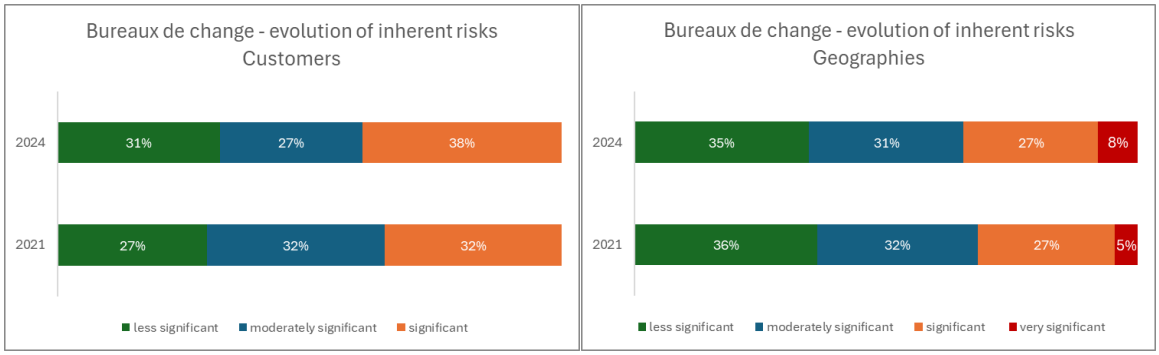


Figure 33: Factors of inherent ML/TF risks in the bureaux de change sector





Life insurance undertakings

In total, 29 CAs responsible for the AML/CFT supervision of LIUs responded to the EBA's questionnaire. Based on the information received from CAs, there are 906 LIUs that are supervised for AML/CFT compliance in the EU. The number of LIUs increased in five MS, while remained stable or slightly decreased between 2021 and 2024.

Figure 34: Inherent ML/TF risks in the life insurance undertakings sector

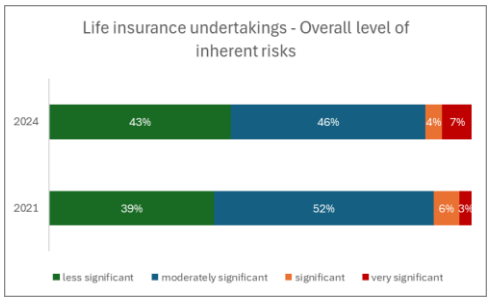
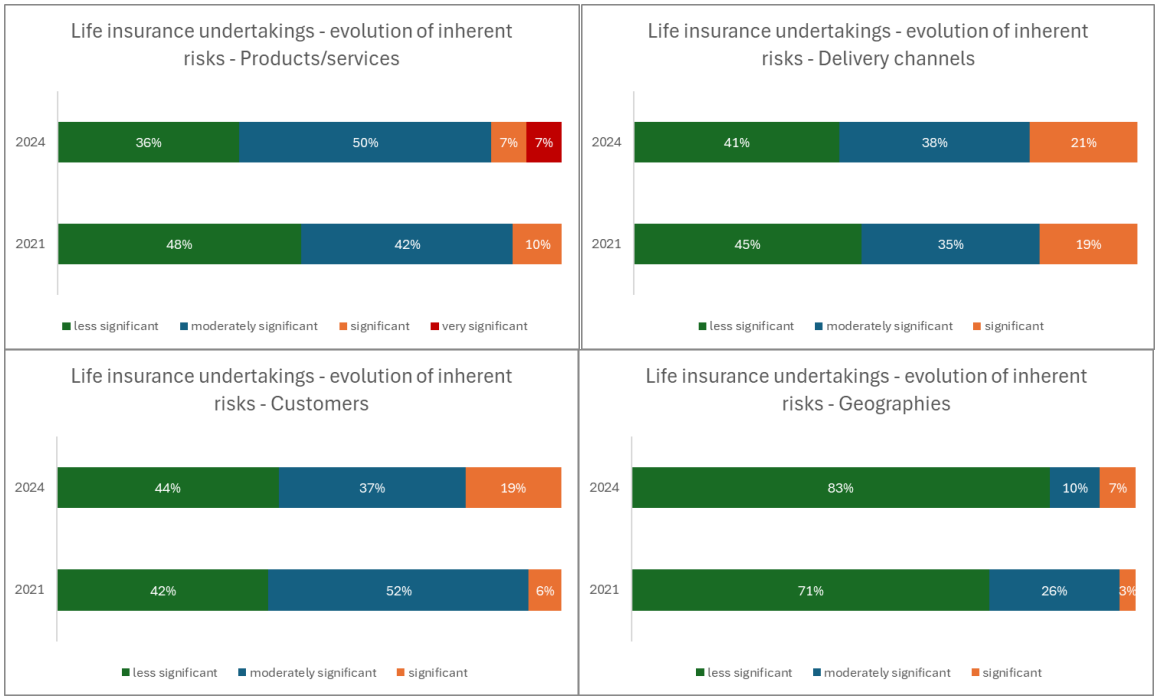


Figure 35: Factors of inherent ML/TF risks in the life insurance undertakings sector



Life insurance intermediaries

In total, 25 CAs responsible for the AML/CFT supervision of 64 995 LIIs responded to the EBA's questionnaire and provided data for 2024. The number of LIIs supervised by the respondent AML/CFT supervisors represent only a fraction of the 796 753 registered insurance intermediaries that were operating at the end of 2022, according to the EIOPA's second report on the application of the Insurance Distribution Directive([33]).

Figure 36: Inherent ML/TF risks in the life insurance intermediaries sector

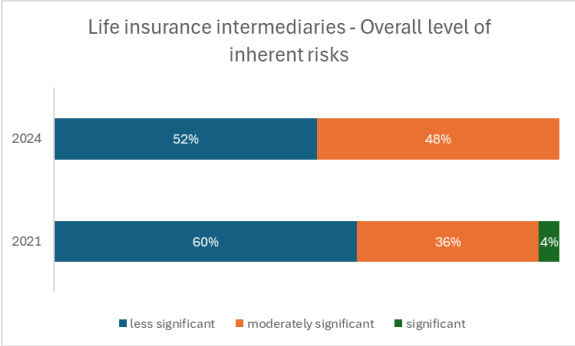
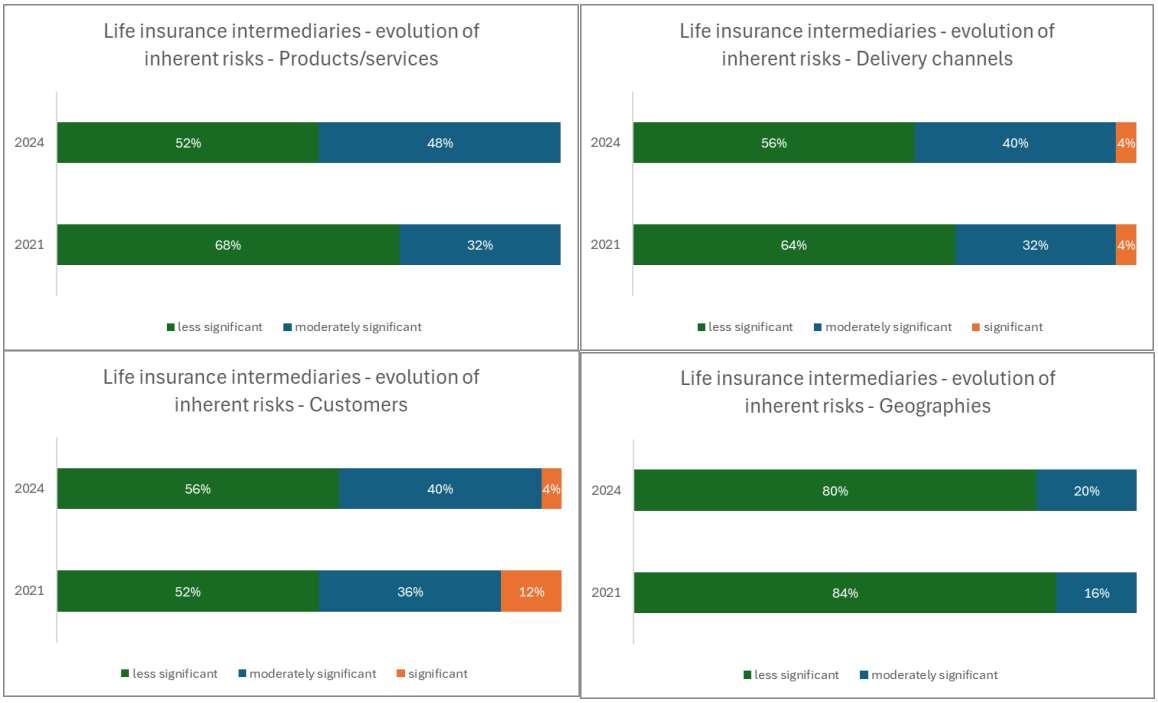


Figure 37: Factors of inherent ML/TF risks in the life insurance intermediaries sector



Investment firms

The EBA received responses from 33 CAs responsible for the AML/CFT supervision of investment firms for 2024, covering a total of 2 971 investment firms. The sector seems rather stable in the number of firms, although one CA saw an increase of 220% and one CA a decrease of 93% in investment firms between 2021 and 2024.

[33] https://www.eiopa.europa.eu/publications/second-idd-application-report-20222023_en.

Figure 38: Inherent ML/TF risks in the investment firms sector

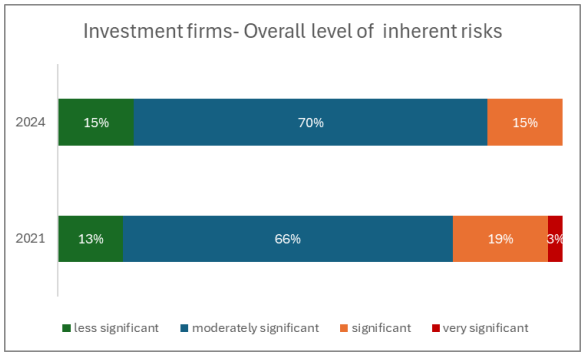


Figure 39: Factors of inherent ML/TF risks in the investment firms sector

Collective investment undertakings

In total, 25 CAs responsible for the AML/CFT supervision of 31 194 collective investment undertakings responded to the EBA's questionnaire in respect of data for 2024. The sector is still highly concentrated, with 72% of the collective investment undertakings located in two Member States. In two other MS, the number of CIUs more than doubled between 2021 and 2024, due to a change of definition between FM and CIU.

Figure 40: Inherent ML/TF risks in the collective investment undertakings sector

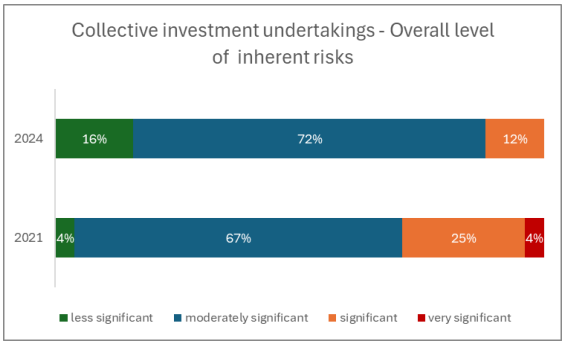
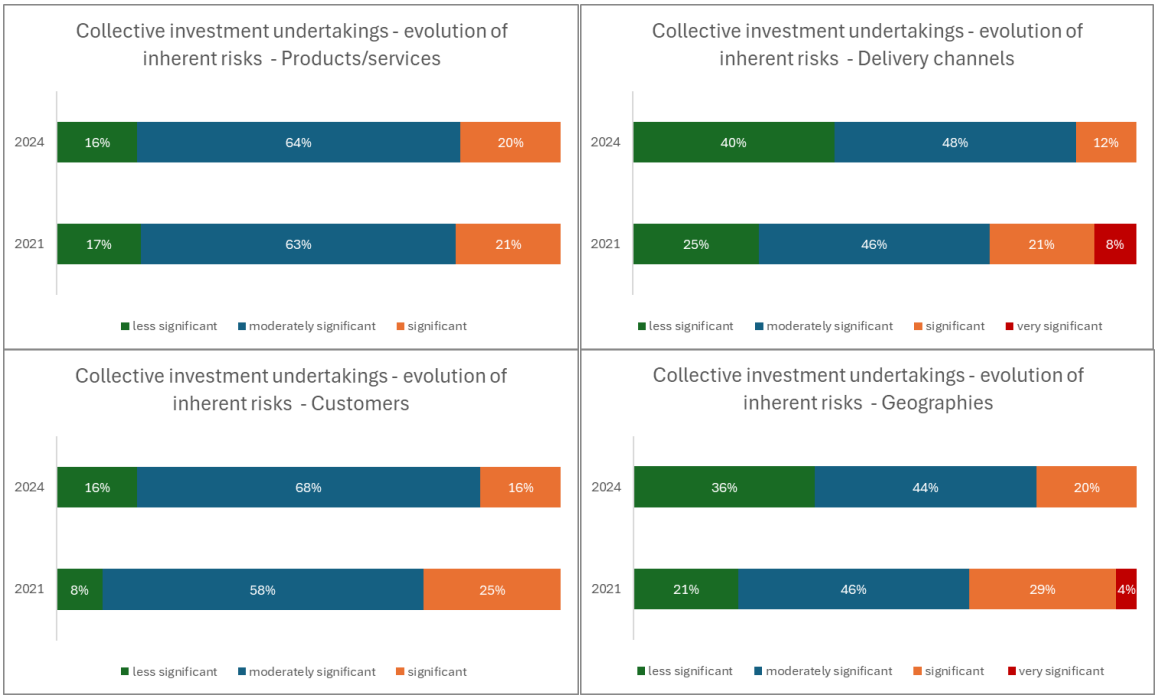


Figure 41: Factors of inherent ML/TF risks in the collective investment undertakings sector



Fund managers

In total, 29 CAs responsible for the AML/CFT supervision of 5 871 fund managers responded to the EBA's questionnaire in respect of data for 2024. The sector is highly concentrated, with almost 60% of all fund managers located in four Member States.

Figure 42: Inherent ML/TF risks in the fund managers sector

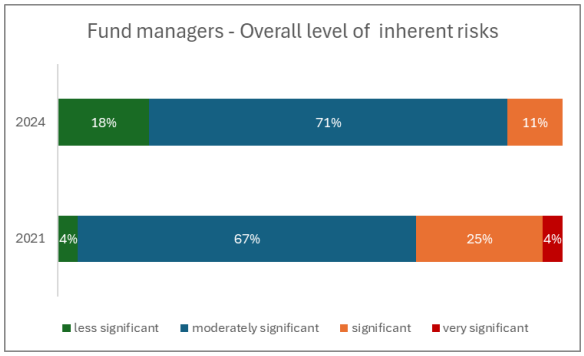
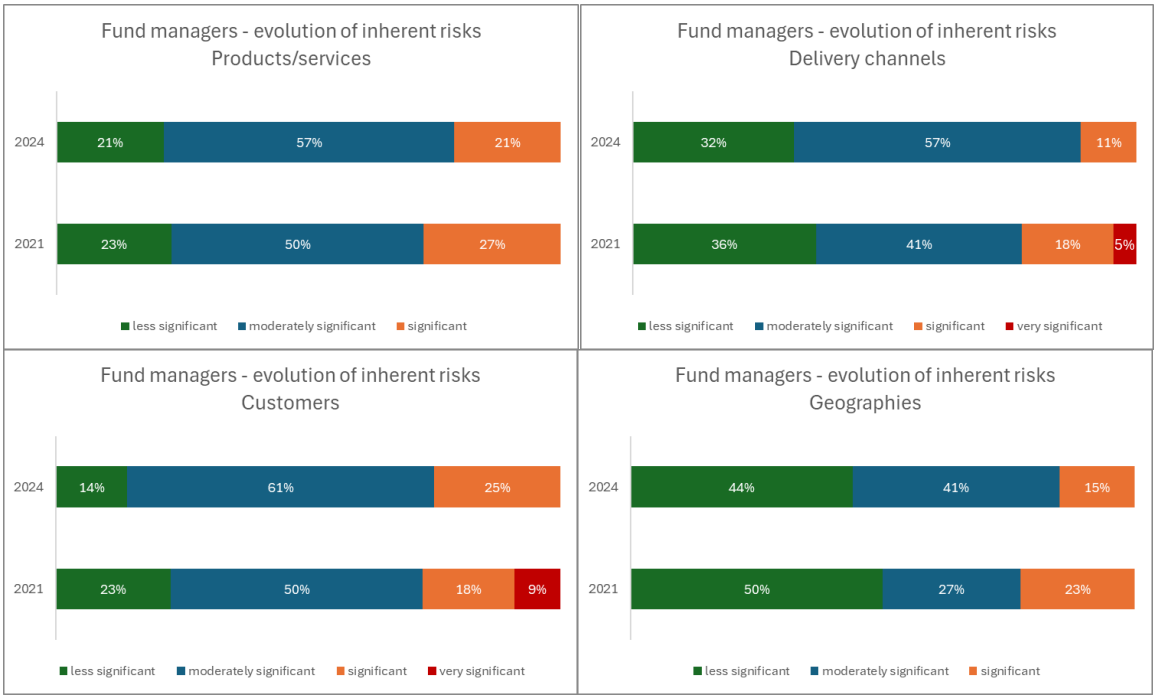


Figure 43: Factors of inherent ML/TF risks in the collective investment undertakings sector



2. Level of residual risks

Figure 44: Evolution of residual risks in the credit institutions sector since 2021

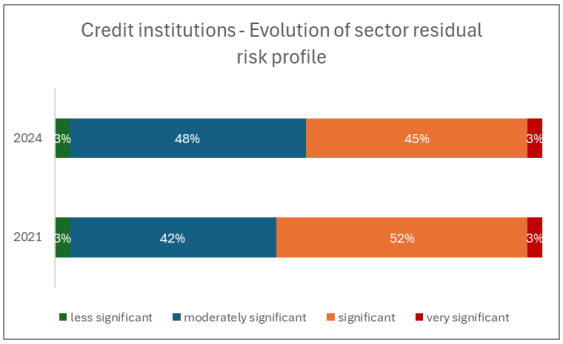


Figure 45: Evolution of residual risks in the payment institutions sector since 2021

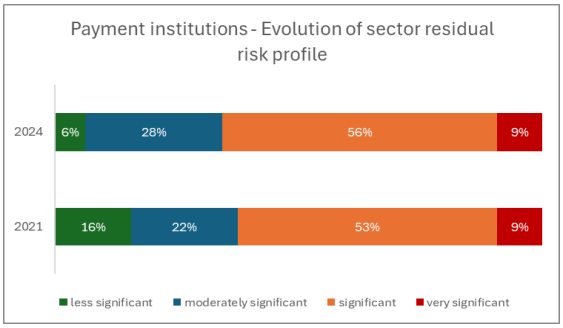


Figure 46: Evolution of residual risks in the e-money institutions sector since 2021

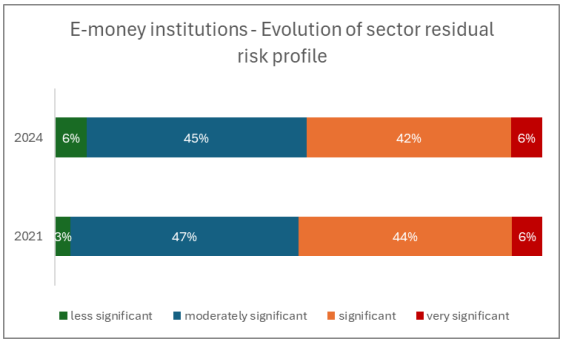


Figure 47: Evolution of residual risks in the crypto asset service providers sector since 2021

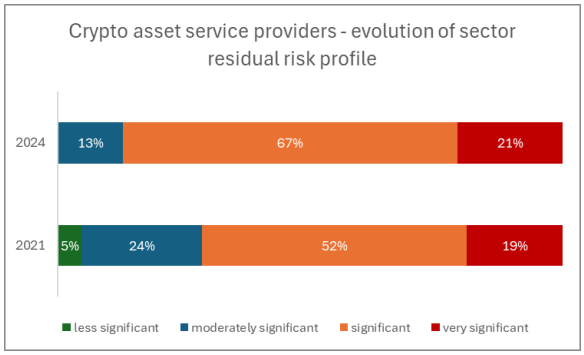


Figure 48: Evolution of residual risks in the credit providers sector since 2021

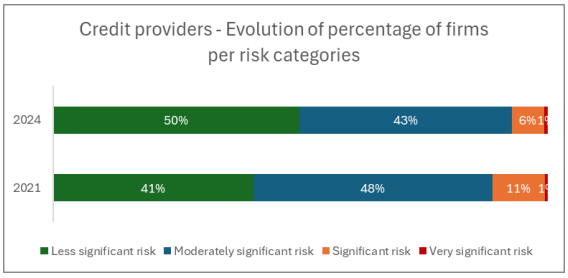


Figure 49: Evolution of residual risks in the bureaux de change sector since 2021

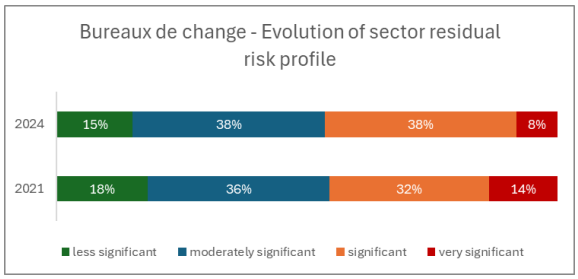


Figure 50: Evolution of residual risks in the life insurance undertakings sector since 2021

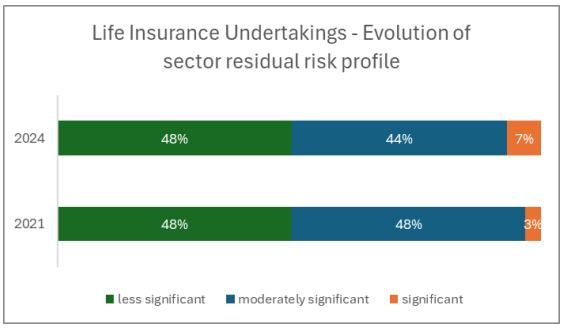


Figure 51: Evolution of residual risks in the life insurance intermediaries sector since 2021

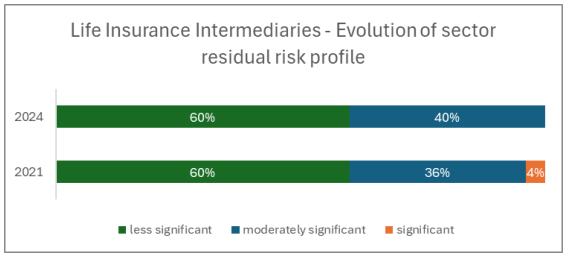


Figure 52: Evolution of residual risks in the investment firms sector since 2021

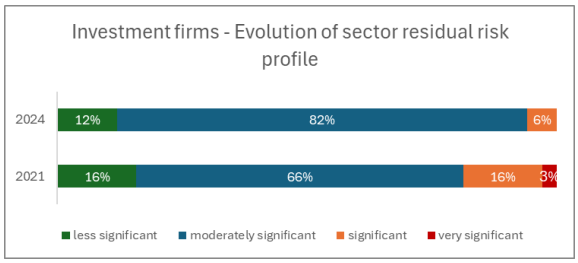


Figure 53: Evolution of residual risks in the collective investment undertakings sector since 2021

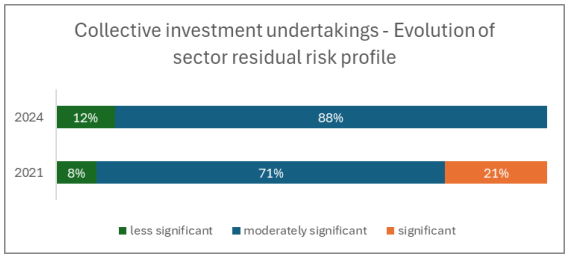
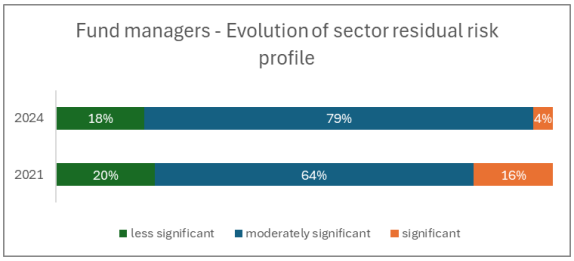


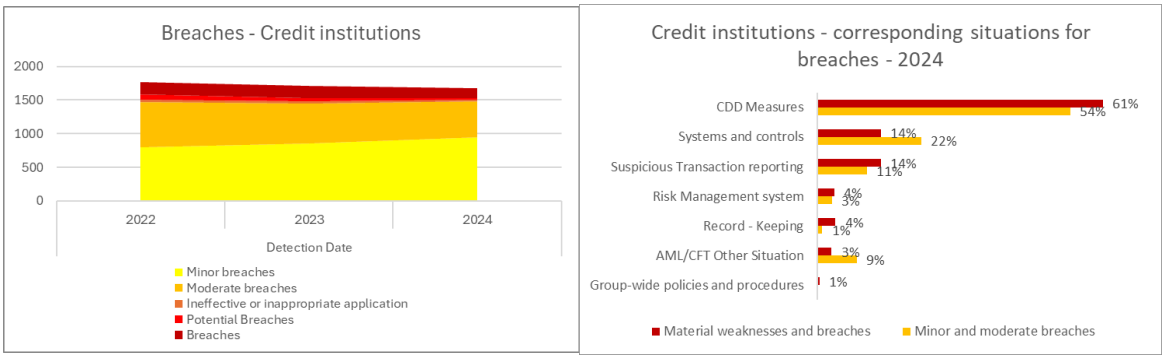
Figure 54: Evolution of residual risks in the fund managers sector since 2021



3. Breaches per sector

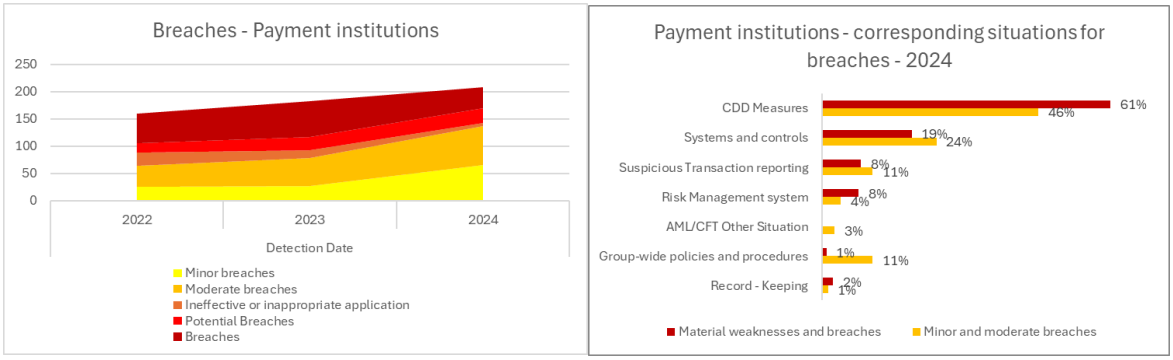
Credit institutions

Figure 55: Breaches and corresponding situations in the credit institutions sector



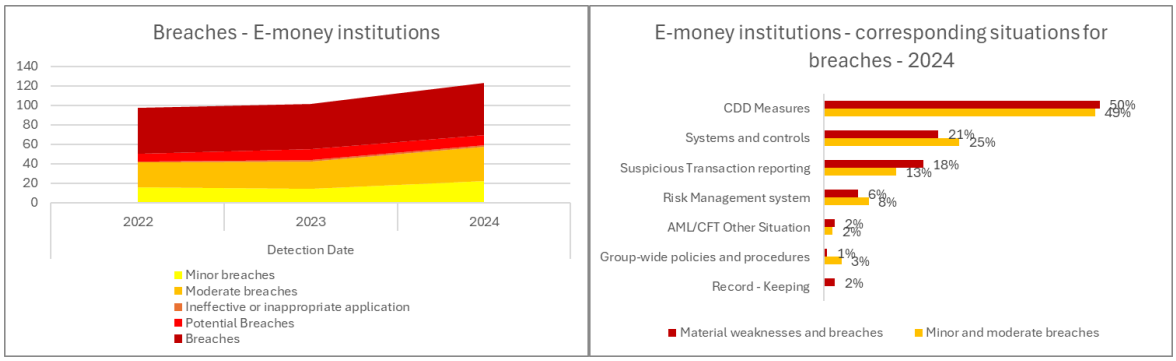
Payment institutions

Figure 56: Breaches and corresponding situations in the payment institutions sector



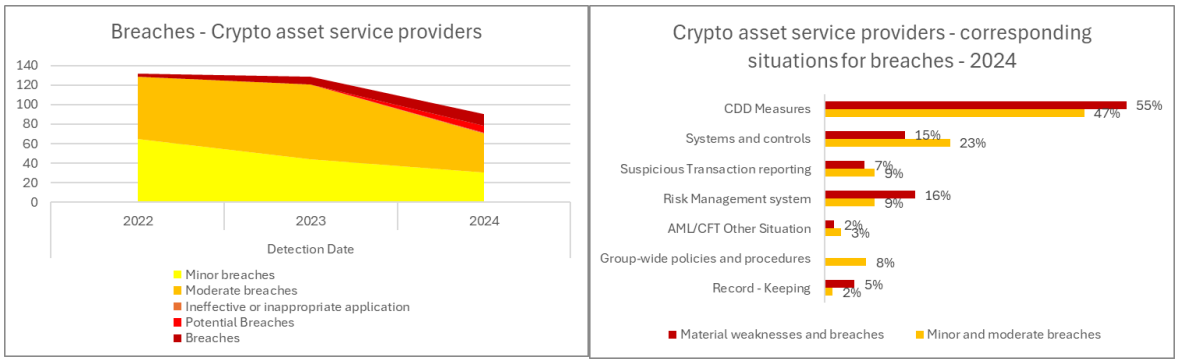
E-money institutions

Figure 57: Breaches and corresponding situations in the e-money institutions sector



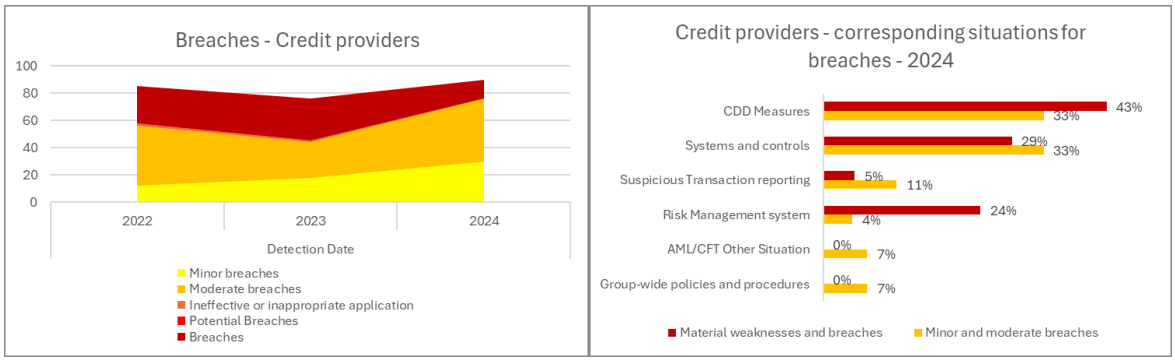
Crypto asset service providers

Figure 58: Breaches and corresponding situations in the crypto asset service providers sector



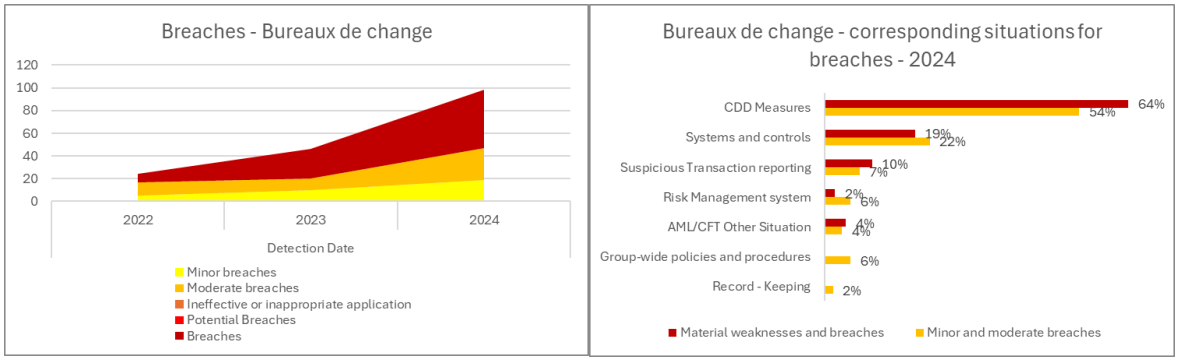
Credit providers

Figure 59: Breaches and corresponding situations in the credit providers sector



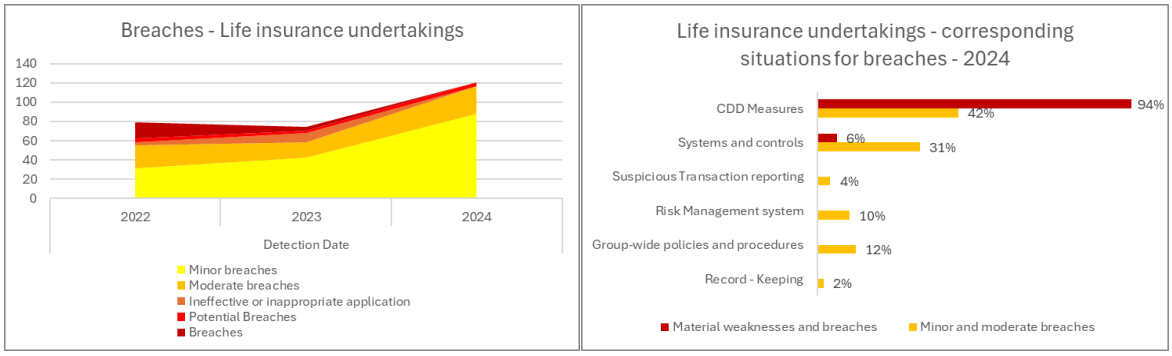
Bureaux de change

Figure 60: Breaches and corresponding situations in the bureaux de change sector



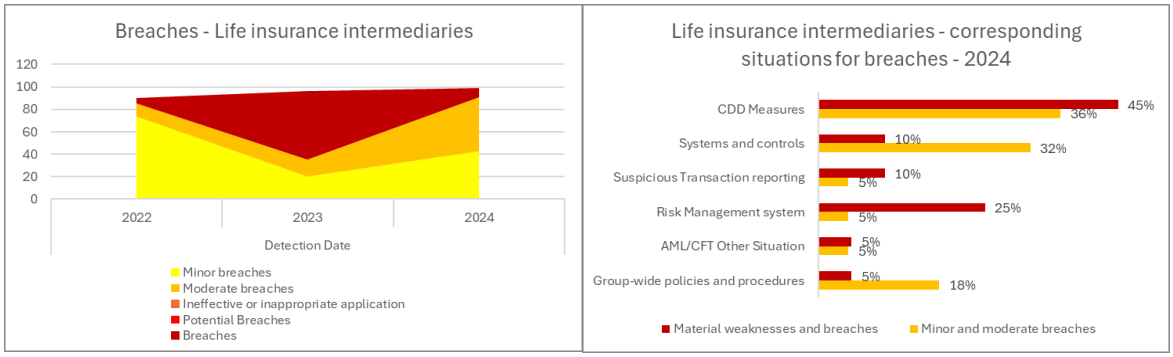
Life insurance undertakings

Figure 61: Breaches and corresponding situations in the life insurance undertakings sector



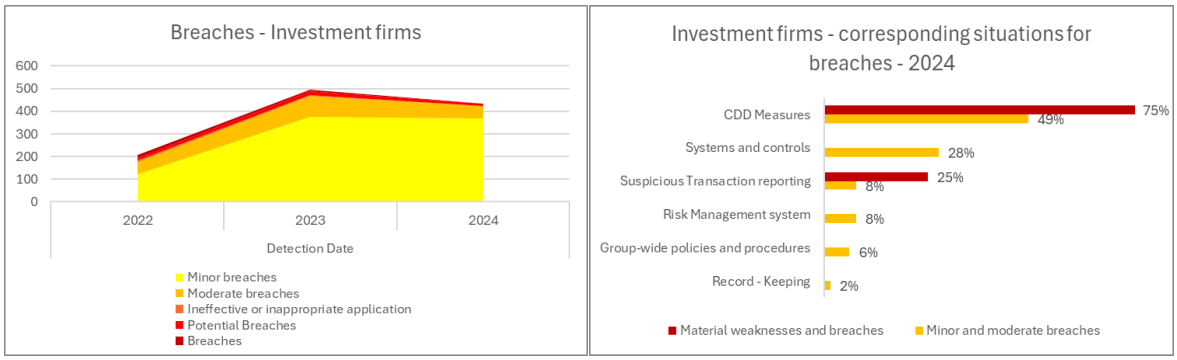
Life insurance intermediaries

Figure 62: Breaches and corresponding situations in the life insurance intermediaries sector



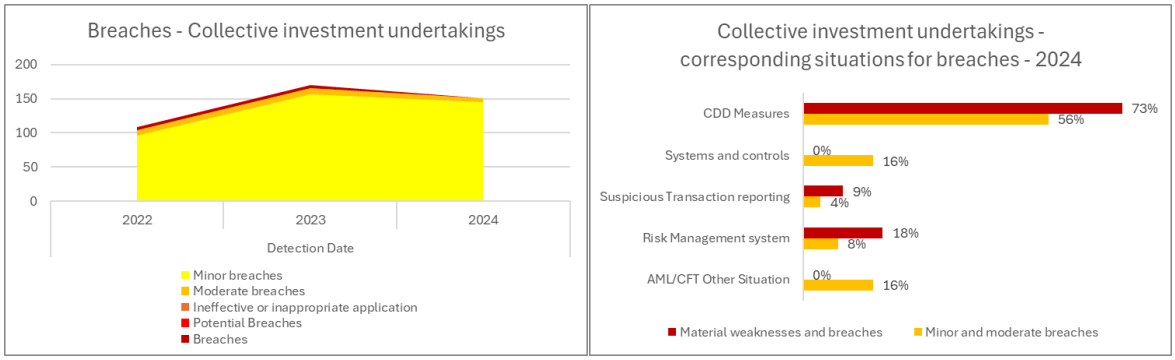
Investment firms

Figure 63: Breaches and corresponding situations in the investment firms sector



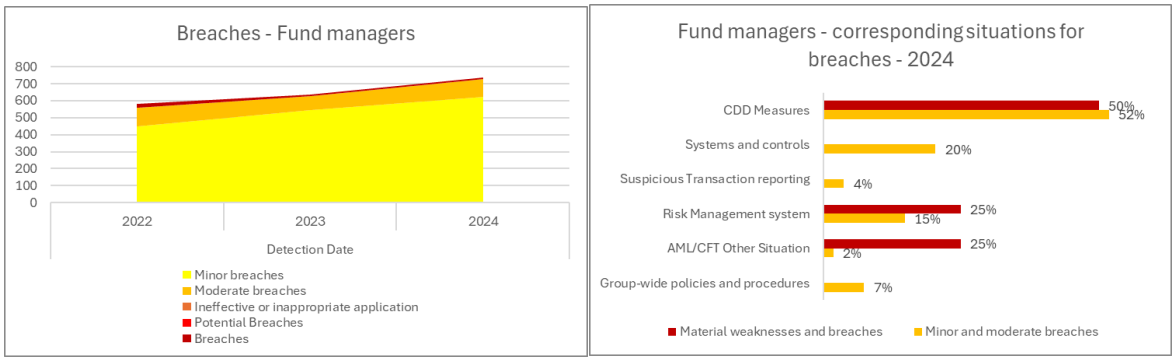
Collective investment undertakings

Figure 64: Breaches and corresponding situations in the collective investment undertakings sector



Fund managers

Figure 65: Breaches and corresponding situations in the fund managers sector



Annex II: Measures undertaken by the competent authorities pursuant to the proposals set forth in the 2023 Opinion

1. In the 2023 Opinion, the EBA issued proposals to the CAs to address risks identified in various sectors. Below are the actions taken by the CAs in response to these recommendations.

Credit institutions

2. CAs supervising CIs were asked to test the effectiveness of key AML/CFT controls in CIs, including transaction monitoring systems and CIs' approaches to identifying and reporting suspicious transactions.

3. Out of the 32 CAs, many provided examples of actions taken to test the effectiveness of key AML/CFT controls. These actions typically began with an assessment of the institution's risk assessment framework, a review of policies and procedures, and an evaluation of the adequacy of internal organisation and resources, including the training of staff. Prior to on-site inspections, CAs often consulted the FIU regarding the quality of STRs and their experience with the institution's compliance department.

4. All CAs reported details on the various types of tests conducted. They noted that they had access to relevant IT systems, such as KYC systems, transaction monitoring systems, and case management systems during on-site inspections.

5. CAs verified that the monitoring systems and rules – both real time and retrospective – were tailored to the institution's business model, customer base, and the products and services offered. They assessed the adequacy of scenarios defined by the entity, including:
   - clients' ML/TF risk classification;
   - appropriateness of thresholds and amounts;
   - consideration of predicate tax offences and TF risks;
   - coverage of current and potential money laundering schemes.

6. CAs examined samples of transactions and cross-checked the scenarios applied by the institution, using both documentation provided and their own analysis of potential ML/TF suspicions. They also conducted statistical analyses of alerts generated for suspicious transactions and evaluated the rate of false positives in relation to STRs submitted to the FIU. Additionally, CAs verified the alert treatment process, including the quality and timeliness of responses. Some CAs inserted fictitious data into transaction monitoring and screening tools to test system effectiveness.

7. Tests were also performed on samples of client files, including closed and refused files, to determine whether suspicious elements were identified and reported to the competent authority. Where applicable, sample testing of cash transactions was conducted to ensure the entity could explain the rationale behind selected transactions.

8. CAs also assessed the adequacy of processes for name screening – particularly for PEPs and targeted financial sanctions – and the escalation of suspicious elements for reporting.

9. CAs have streamlined procedures for selecting samples of customers, respondent entities and transactions. These procedures depended on the scope of the inspection (aiming for a representative sample) and the nature and size of the entity. One CA reported developing an in-house tool to enable more efficient and effective risk-based sampling of client transactions.

10. Effectiveness was further tested through interviews with employees or responsible persons to assess compliance with the AML/CFT framework. Some CAs conducted virtual walkthroughs of IT systems and procedures, enhancing the intrusiveness of off-site supervision.

11. In the case of financial groups, CAs reviewed whether processes such as transaction monitoring – when handled at the group level – were appropriately followed up by individual entities within the group in the event of deficiencies.

12. Some CAs also performed virtual walkthroughs of IT systems and procedures, which increased the intrusiveness of off-site supervision.

13. Thirty-one percent (10) of the CAs provided details on recent thematic inspections or reviews. These covered areas such as:
    - targeted financial sanctions;
    - new transaction monitoring tools;
    - outsourcing;
    - virtual IBANs;
    - de-risking;
    - t detection;
    - remote onboarding;
    - private banking;
    - annual self-assessment procedures;
    - evaluation of technical and human resources;
    - identification of PEPs and implementation of EDD measures;
    - beneficial ownership identification;
    - cash transaction reporting;
    - scrutiny of correspondent relationships;
    - risks associated with citizenship and residency-by-investment.

Payment institutions

14. CAs supervising PIs were asked how they provided specific guidance to the sector to ensure that supervisory expectations regarding adequate and effective AML/CFT systems and controls are well understood and applied.

15. Out of the 31 CAs, four conducted off-site targeted or thematic reviews to assess the adequacy and effectiveness of key AML/CFT controls. These included transaction monitoring, PSPs providing services to clients with sub-merchants, and the supervision of agents by various PIs

engaged in money remittance. Feedback was provided either individually or through aggregated findings and best practices published in a report.

16. Eight CAs reported that on-site engagements with AML Compliance Officers were more effective than general guidance, as they allowed for a better understanding of the sector's diverse business models and AML/CFT frameworks.

17. Six CAs viewed targeted on-site inspections as an opportunity to provide guidance on supervisory expectations. These inspections offered direct supervisory feedback and guidance to strengthen AML/CFT controls. The publication of enforcement measures also served as guidance on regulatory requirements.

18. 12 CAs organised conferences or training sessions to present risk factors and highlight deficiencies identified during supervisory activities.

19. 12 CAs updated their guidelines and other communication tools (e.g. risk letters or annual reports). These updates included guidance notes on transaction monitoring, the travel rule, and money laundering and TF risks arising from migrant smuggling, particularly in countries serving as transit points for illegal migration. Two CAs emphasised the importance of providing guidance to PIs on conducting business-wide risk assessments.

20. CAs were also asked to take actions to ensure a sufficiently risk-based and intrusive supervision, in line with provisions in the Risk-based AML/CFT Supervision Guidelines. Two CAs reported that they had not taken any action.

21. Thirteen CAs collected comprehensive information on business models and specific risk indicators. For example, CCP reports included various quantitative and qualitative data points, such as the number and main reasons for, as well as details on, registered PIs (e.g. internal reports submitted, number and volume of transactions). Data were also collected annually for sectoral risk assessments, with new questions introduced to address emerging risks – such as the use of virtual IBANs. The methodology assessed these indicators in relation to activities in other countries (either through establishment or service provision), with data analysed separately per country.

22. Two CAs monitored emerging risks on a quarterly basis and updated their risk ratings throughout the year as new information becomes available. Interactions with high-risk PIs regarding their business models and product offerings led one CA to conduct further in-depth analysis on specific technical topics, such as virtual IBANs and the use of AI.

23. One CA engaged an external consultancy firm to support the development of its strategy for regulating, licensing and supervising PIs/EMIs, and to enhance its supervisory approach across the full lifecycle of the PI/EMI sector.

24. Twenty-two percent (7) of CAs favoured thematic reviews, focusing on areas such as:
    - money remittance corridors;
    - online business relationship establishment and transactions without customer presence;
    - PEPs and sanctions controls;
    - rules and procedures for establishing the source of funds and wealth;
    - systems for ongoing and transaction monitoring;
    - oversight of agent activities.

25. Thirty-nine percent (12) of CAs reported conducting on-site inspections of the riskiest PIs, sometimes followed by flash missions. These inspections allowed CAs to examine IT systems in depth, including advanced testing of automated controls. For high-risk entities, the level of sampling was increased, with more tests and larger sample sizes. Some AML/CFT inspections were conducted jointly with IT experts capable of reviewing programming code. Targeted on-site inspections focused on higher-risk areas such as:
    - scrutiny of correspondent relationships;
    - adequacy of onboarding procedures and agent training;
    - oversight actions based on the ML/FT risk of agents;
    - assessment of filtering and monitoring systems implemented locally in agent networks.

26. Finally, CAs were also requested to take actions to focus more on the supervision of agent networks and to cooperate more with their counterparts in case of cross-border agent networks. Three CAs reported taking no action. One CA emphasised the ambiguity in the new AML package, noting that it does not resolve the issue whereby host supervisors are expected to oversee activities conducted by institutions not under their direct supervision, through entities that have no legal obligations.

27. One CA developed internal guidelines for supervising payment agents based on their risk profile. Payment agents deemed significantly high-risk – such as those contracted with multiple PIs, those with a high volume or a sharp year-on-year increase in funds transferred, or those flagged by public prosecutors – were required to complete a detailed questionnaire to assess their ML/TF-related data.

28. Thirteen percent (4) of CAs focused on the oversight of PI agent networks by issuing guidelines on due diligence prior to entering into business relationships with agents. These guidelines also required maintaining a detailed register of agents, including ownership structures, key management personnel and business locations. Another CA conducted a thematic review on the use of agents in PI business models, focusing on risks, weaknesses and best practices in agent selection, assessment, monitoring, control and training. The findings were communicated to the relevant entities, which were asked to submit action plans to strengthen their agent-related policies and procedures. Another CA published a typology paper on unregulated businesses within payment agent networks, including a threat assessment.

29. Thirty-two percent (10) of CAs conducted on-site inspections of agents for both domestically authorised and foreign PIs. Thirty-eight percent (12) of CAs reported sharing information through AML/CFT Colleges of PIs, particularly regarding agent oversight and training. Additionally, 13% (4) of CAs carried out joint supervisory actions for cross-border agent supervision. These actions aimed to (i) map ML/TF risks related to agents and distributors of PIs, and (ii) assess whether the conditions under Article 29(4) of PSD2 were met to require the appointment of a central contact point.

30. One CA organised physical AML/CFT visits to the shared service centres of two PIs to better understand the effectiveness of outsourced controls. These visits included the supervised entities and other supervisory authorities. Three other CAs shared specific data on agent networks and complaints related to agent activities for represented entities.

31. Thirteen percent (4) of CAs held annual meetings with the AML/CFT central contact points established by entities that meet the relevant requirements.

E-money institutions

32. CAs supervising e-money institutions were asked to adjust their supervisory plans – both on-site and off-site – according to the ML/TF risk profile of individual e-money institutions, and on the ML/TF risks in that sector. Out of the 31 CAs, three reported taking no specific action.

33. Ten percent (3) of CAs reported improved use of information for risk assessment, such as implementing a new methodology to analyse the annual reports submitted by AML Compliance Officers (AMLCOs). Another CA conducted an annual targeted AML/CFT survey to gather key risk information from EMIs with a 'significant' or 'very significant' risk profile. This included additional data on the implementation of specific AML/CFT systems (e.g. selected internal regulations, audit activity reports).

34. Ten percent (3) of CAs facing increased risks – due to a higher number of authorised EMIs, EMIs operating through agent networks, new FinTech business models, or a higher risk appetite in accepting clients typically rejected by traditional banks – adjusted their supervisory plans. These adjustments included more frequent exchanges, communications, and meetings with the concerned entities, as well as more targeted on-site inspections. For example, one CA focused its on-site inspections on money remitters with the highest transaction volumes to high-risk countries.

35. Sixteen percent (5) of CAs revised their risk assessment methodologies to evaluate risk indicators related to cross-border activities (either through establishment or service provision), with assessments conducted separately for each country. This led to a supervisory visit to a single high-risk entity (responsible for over 90% of sector transactions) and numerous intrusive off-site reviews for nearly all other companies. Another CA enhanced its supervisory approach for the EMI sector across its full lifecycle.

36. In 13% (4) of CAs, where EMIs with low or medium risk scores are not subject to annual on-site supervision, all EMIs are still subject to annual or biennial off-site supervision. This is conducted through questionnaires, annual bilateral meetings and supervisory dialogues. In one CA, where the number of supervised EMIs had decreased, the authority was able to organise more dedicated meetings with AMLCOs and internal audit functions. Twenty percent (6) CAs indicated they have close cooperation with the FIU to discuss the modus operandi of e-money agents, individual risk profiles of EMIs and areas to focus on during on-site inspections.

37. Twenty percent (6) of CAs reported close cooperation with their FIUs to discuss the modus operandi of e-money agents, individual EMI risk profiles, and areas of focus for on-site inspections.

38. Thirty percent (6) of CAs conducted thematic reviews on topics such as:
    - anonymous e-money;
    - risks and controls associated with 'Golden Visa' customers;
    - neo-banks;
    - remote onboarding;
    - branches and central contact points of EU EMIs.

39. During on-site inspections, two CAs performed advanced testing of automated controls (e.g. transaction monitoring and name matching), analysed large datasets, and reviewed programming code.

40. CAs were also requested to provide specific guidance to the sector to ensure that supervisory expectations regarding adequate and effective AML/CFT systems and controls are well understood and applied.

41. Forty-two percent (13) of CAs organised conferences or training sessions for representatives of EMIs to cover identified ML typologies, good practices and deficiencies identified during supervisory activities, or more technical topics such as virtual IBANs.

42. Twenty-two percent (7) of CAs provided guidance based on observations from on-site inspections or thematic reviews. Topics included targeted financial sanctions, risk analysis, transaction monitoring, weaknesses and best practices related to the use of agents by PIs, and aggregate statistics on ML/TF sectoral risk indicators.

43. Ten percent (3) of CAs favoured tailored guidance approaches, such as bilateral meetings, particularly in cases where the sector was small or business models varied significantly.

44. Forty-eight percent (15) of CAs recently updated their AML handbooks or issued new communications and guidelines. These addressed topics such as CDD for AIS and payment initiation services, sanctions risk assessments, EDD measures related to TF, the use of technology for transaction monitoring, and the application of the Instant Payments Regulation.

Crypto asset service providers

45. CAs supervising CASPs were asked to ensure that their staff receive adequate and up-to-date training to have the technical skills and expertise necessary for the execution of their functions.

46. All 23 CAs indicated that they ensured their staff attended training sessions. All CAs reported that their staff participated in external training, either provided by private companies or through workshops organised by EU authorities such as the EBA, ESMA, Europol, and the EU Supervisory Digital Finance Academy (EU-SDFA). One CA also mentioned recruiting staff with a background in crypto assets. The topics covered included:
    - types of crypto asset business models and decentralised finance;
    - ML/TF risks associated with these business models;
    - advanced blockchain analytics tools to support client onboarding and transaction monitoring;
    - training on the legal frameworks of the FTR and the MiCA.

47. To strengthen internal expertise, some CAs recruited staff with crypto-related backgrounds and created working groups to share knowledge. Four CAs reported receiving training from the FIU or the judicial police. One CA is part of a permanent national working group on crypto assets alongside other authorities. Two CAs stated they had exchanged experiences with other supervisors at EU or international level.

48. CAs were also requested to focus their risk assessment on areas identified in the amendments to the EBA's Risk Factors Guidelines and the amendments to the Guidelines on information requirements in relation to transfers of funds and certain crypto asset transfers under Regulation (EU) 2023/1113.
49. Thirty-five percent (8) of CAs had not yet taken any action, citing reasons such as the Fund Transfer Regulation not being applicable before the end of 2024, the appointment of a new CASP supervisor in 2025, or the absence of licensed CASPs.

50. Twenty-one percent (5) of CAs updated their questionnaires or risk classification methods to incorporate new risk factors, such as the identification of self-hosted wallets. One CA collected information on crypto asset addresses controlled by its registered CASPs. These data were used in a blockchain analysis tool to better understand the ML/TF risks associated with the crypto asset sector. Twenty-one percent (5) of CAs conducted new sectoral risk assessments, taking into account the EBA's updated Risk Factor Guidelines.

51. Thirteen percent (3) of CAs enhanced their scrutiny of fitness and propriety, business models and AML controls of CASPs applying for authorisation. In each new registration, the CA imposed supervisory measures – mostly orders and requests for additional information – delaying the commencement of operations. Eight percent (2) of CAs plan to assess the implementation of the travel rule in 2025 through full-scope on-site inspections or thematic reviews.

Credit providers

52. CAs supervising CPs were asked to identify the main risks in each subsector of CPs and focus their supervisory activities on areas representing the highest ML/TF risk.

53. Of the 26 CAs: 23% (6) of CAs did not take any specific actions. All other CAs use off-site analysis to target higher-risk areas, such as institutions operating in international leasing and factoring, or non-performing loan managers. Nineteen percent (5) of CAs used the AML questionnaire, incorporating some newly monitored data points, to identify main risks.

54. Thirty-five percent (9) of CAs carried out their first sectoral risk assessment or updated it, including an assessment of sub-sectors. One CA used quantitative evidence from AML Questionnaires, prudential supervision reports, and data from the FIU. Another CA conducted the sectoral risk assessment with other authorities like the FIU, law enforcement and tax authorities. Five CAs reviewed their risk assessment methodologies and planning, using additional statistical information from consumer complaints, from prudential supervisors on licensed consumer credit provider sector and public registers focused on the most significant risks.

55. One CA requested information from institutions to gain a deeper understanding of the business models of those operating in international factoring. Consequently, the AML and prudential supervisors of leasing and factoring institutions have established a new format for information exchange between AML and prudential supervisors.

56. Nineteen percent (5) of CAs carried out extensive off-site reviews of higher risk types of CPs (e.g. credit servicing firms and specialised CIs). Risks related to staff were assessed in cooperation with prudential supervisors, either as part of the AML risk assessment or a relicensing process for all entities.

57. Eleven percent (3) of CAs carried out licensing or relicensing procedures. One CA conducted a licensing process for non-performing loan managers, including an assessment of internal AML regulations, and is currently preparing a risk assessment. In another MS, all consumer CPs other than CIs came under the supervision of a new authority. During the re-registration of consumer CPs, the new CA reviewed all AML/CFT materials and remediated identified shortcomings.

58. One CA shifted from thematic inspections, which covered more sectors but only partial aspects, to a more focused approach. For the 2024 plan, an analysis of larger CPs estimated their risk as low. Nonetheless, the largest CFI (dedicated to non-specialised consumption) was included in the 2024 inspection plan.

59. Another CA conducted numerous intrusive or analytical off-site assessment reviews before on-site inspections, creating synergies between ML risk and credit risk management systems, and transaction monitoring for specific typologies related to loan use, real estate collateral and loan repayments.

Bureaux de change

60. CAs supervising bureaux de change were asked to ensure a sufficiently broad view of AML/CFT systems and controls, especially where bureaux de change offer other services such as gold and precious stones trading.

61. Of 26 CAs supervising bureaux de change, 15% (4) of CAs took no action and 27% (7 CAs) reported that their supervised bureaux de change did not offer additional services such as trading gold and precious stones. All CAs collected data through the annual AML/CFT questionnaire, with some adding specific questions about other high-risk activities.

62. Thirty-five percent (9) of CAs have updated or are updating their sectoral risk assessments. As a result, one CA noted an expansion in branch networks and services (including gold and precious stones trading and money transfers), raising the sector's overall AML/CFT risk from 'medium' to 'medium-high'. In four MS, all bureaux de change involved in gold and precious metals trading were assigned a high risk level and received intensified or additional supervision.

63. Fifteen percent (4) of CAs had conducted additional supervision since 2023:
    - One CA had performed full-scope unannounced on-site inspections, considering the entire sector high-risk.
    - Another CA had conducted a thematic review of currency exchange offices, selecting 15 entities in a first phase, and inspecting four of them in a full-scope inspection. Breaches were identified in all four bureaux de change and reported to EuReCA.
    - One CA carried out off-site reviews, assessing AML/CFT frameworks across multiple financial activities.
    - Another CA carried out a cycle of on-site inspections and published a report on deficiencies identified.

64. These supervisory activities have led to legislative and guideline updates:
    - In two MS, new legislation was being considered to restrict the provision of currency exchange services to some financial institutions or to amend the AML/C F T Law for a risk-adjusted due diligence threshold.
    - Two CAs updated their guidelines, with one publishing joint guidelines with customs on gold and precious metals trading in 2024.

Life insurance undertakings

65. CAs supervising LIUs were asked to address identified weaknesses in controls, such as customer identification and verification related to beneficial owners and PEPs.

66. Of the 29 CAs responsible for the AML/CFT supervision of LIUs, three did not take any actions.

67. Twenty percent (6) of CAs confirmed their sectoral risk assessment as low-risk, with minimal or no identified weaknesses in controls, and with few inherent risks, such an exposure of 0.26% to

PEPs for stock of insurance contracts. In several cases, the fact that half of LIUs are part of credit institution groups is considered a risk mitigating factor. Two other CAs performed a sectoral risk assessment in 2022–2023, either as dedicated exercise for life insurance companies, or as part of the national risk assessment.

68. Regarding off-site actions, 20% (6) of CAs use their annual AML/CFT questionnaire to monitor the sector. Seventeen percent (5) of CAs conducted targeted reviews: one CA requested information from all branches of primary insurance undertakings to understand the scope and nature of their business. One other CA focused on customer profiling and transaction monitoring in cases of early redemption.

69. Twenty-four percent (7) of CAs carried out on-site inspections in high-risk entities, focusing on the effectiveness of KYC processes, PEP-screening systems, and identification of beneficial ownership. One CA identified deficiencies in key AML/CFT controls related to customer identification and verification in most on-site inspections conducted in 2023 and 2024. Consequently, these supervised entities were instructed to develop an appropriate remediation plan. Seventeen percent (5) of CAs updated their guidance to the sector following their supervisory actions.

Investment firms

70. CAs supervising investment firms were asked to provide specific guidance to the sector to ensure that supervisory expectations regarding adequate and effective AML/CFT systems and controls are well understood and applied. Of the 33 CAs, 12% (4) did not take any action.

71. Eighteen percent (6) of CAs conducted off-site targeted or thematic reviews on AML safeguards, such as AML governance, internal controls, and the risk-based approach adopted by investment and asset management companies. Feedback was provided individually, or aggregated findings were sometimes made public in a report.

72. Twelve percent (4) of CAs explained that they used on-site engagements with AMLCOs to better understand business models and AML/CFT frameworks, delivering key messages on an individual basis. These engagements helped identify difficulties encountered in practice. As a result, one CA organised an AMLCO day to provide guidance to the whole sector.

73. Thirty-three percent (11) of CAs considered on-site inspections as an opportunity to provide guidance on supervisory expectations. One CA conducted thematic inspections to evaluate controls implemented by investment firms operating online trading platforms, due to increased risks associated with remote onboarding of customers. Post-inspection feedback was considered the most important part of these inspections.

74. Thirty-six percent (12) of CAs organised conferences or training for their supervised sector to discuss difficulties encountered and possible solutions, to provide insights into the results of the NRA relevant to the sector and present key takeaways from AML/CFT supervision (both on-site and off-site) with some best practices related to AML/CFT legal requirements. One CA organised training on the notion of client for UCI management companies and the duties of ongoing vigilance towards clients.

75. Thirty-three percent (11) of CAs updated their guidelines, handbooks or Q&A documents, highlighting vulnerabilities specific to investment firms sector and providing recommendations.

These documents addressed common weaknesses/deficiencies identified during on-site/off-site supervision.

Collective investment undertakings

76. CAs supervising collective investment undertakings were requested to base the frequency and intensity of on-site and off-site supervision on the ML/TF risk profile of individual collective investment undertakings, and on the ML/TF risks in that supervised sector. Of the 35 CAs, four CAs did not take in action.

77. Twenty percent (7) of CAs updated their questionnaires and risk assessment methodologies to collect statistical information from all supervised entities and to identify new or emerging ML/TF risks. One CA introduced new supervisory tools, including checks against beneficial ownership registers and adverse media monitoring, to more effectively capture emerging threats. Another CA created a dedicated section for closer oversight tailored to cross-border structures and extended reporting requirements to include national funds managed by foreign fund managers. One CA also adjusted the frequency of its periodic AML/CFT questionnaire, moving from an annual to a biennial schedule.

78. Thirty-seven percent (13) of CAs indicated that they adjusted the focus, scope and frequency of both off-site and on-site supervision where the assessed risk was higher compared to peer obliged entities. In addition to full-scope investigations based on risk assessment outcomes, one CA placed greater emphasis on thematic investigations – for example, focusing on UBOs and PEPs.

79. One CA explained that it categorised the 'asset management companies' sector into four sub-sectors. Three sub-sectors cover domestic asset management companies, differentiated by the nature of the funds managed (open-end, closed end, and real estate), while the fourth includes all branches of foreign asset management companies. Among these, only the real estate funds sector was assessed as having a significant risk rating.

80. Another CA concentrated its AML/CFT supervisory resources on Fund Administrators and Depositaries, recognising their gatekeeper role and the high level of outsourcing by funds and fund managers to these entities for executing AML/CFT control frameworks.

81. Finally, three CAs provided guidance to CIUs based on findings from both on-site and off-site supervision.

Fund managers

82. CAs supervising fund managers were asked to take actions to address identified weaknesses in controls, particularly regarding the oversight of AML/CFT frameworks implemented by fund managers. Of the 29 CAs, five reported taking no action.

83. Ten percent (3) of CAs used reporting requirements to follow up on identified weaknesses in fund managers. These were also used to trigger further supervisory measures or more intrusive enforcement actions if the corrective measures implemented by fund managers proved ineffective. One of these CAs extended this preventive reporting to locally based funds managed by foreign fund managers, allowing for closer oversight tailored to cross-border structures. This

CA also developed new supervisory tools, including beneficial ownership register checks and adverse media monitoring, to better capture emerging threats.

84. Seventeen percent (5) of CAs conducted targeted off-site reviews of fund managers, focusing on specific high-risk topics such as AML governance and internal controls, the risk-based approach, and compliance with targeted financial sanctions.

85. Two CAs favoured supervisory engagements with the AMLCOs of fund managers to assess various control areas, including oversight of the AML/CFT framework. These engagements also helped determine whether further firm-level or sectoral engagement was needed. Additionally, they were used to better understand the practical challenges faced by AMLCOs and to take note of requests for clarification of supervisory expectations.

86. Thirty-four percent (10) of CAs conducted on-site inspections – whether full-scope, targeted or thematic. These inspections tested the effectiveness of CDD and ongoing monitoring using sample reviews. They also assessed whether the AMLCO had sufficient authority and resources to perform their duties effectively. One CA conducted a targeted review focused on customer risk assessment, customer profiling and transaction monitoring. Two CAs noted that post-inspection letters of recommendation also served as guidance to help the obliged entities address identified shortcomings.

87. Twenty-seven percent (8) of CAs provided awareness-raising and training activities to strengthen controls and risk management. For example, they shared sectoral analyses on topics such as the higher ML risk associated with investment funds exposed to real estate and residency-by-investment schemes, the definition of a client for UCI management companies, and the obligations of ongoing vigilance toward clients.

European Banking Authority

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE
Tel. +33 1 86 52 70 00

E-mail: info@eba.europa.eu

https://eba.europa.eu