EBA/Op/2023/08

13 July 2023

EBA Regular Use

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 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, Articles16a(1) and 29(1) (a) of Regulation (EU) No 1093/2010[1], which requires the EBA to issue such an Opinion every 2 years. This Opinion serves to inform competent authorities' application of the risk-based approach to anti-money laundering (AML) / countering the financing of terrorism (CFT) supervision and the European Commission's Supranational Risk Assessment. It is addressed to the European co-legislators and AML/CFT competent authorities.

2. This is the EBA's fourth Opinion on ML/TF risks. It is based on data from January 2020 to January 2023, including 49 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.

3. 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.

[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).

4. In accordance with Article 14(7) of the Rules of Procedure of the Board of Supervisors[2], the Board of Supervisors has adopted this Opinion.

General comments

5. Since the EBA's third Opinion on ML/TF risks was published in 2021, geopolitical events and technological advances have had a profound impact on the financial sector's exposure to financial crime risks. Russia's invasion of Ukraine in February 2021 led to the imposition by the EU of restrictive measures that are unprecedented in terms of their scale and their scope, but national approaches to enforcing restrictive measures are not harmonised and create pressure on institutions' compliance resources. At the same time, the risk of financial institutions being used to circumvent sanctions has increased. The large-scale displacement of vulnerable persons from Ukraine has led to a surge in human trafficking and given rise to an urgent need to provide access to financial services to refugees from Ukraine. New risks arise from the laundering of proceeds from environmental crimes and cybercrimes, with a perceived increase in risks associated with financial innovation linked to market growth. Legislative developments, including a comprehensive 'AML Package' and the Markets in Crypto-Assets Regulation create legal uncertainty and a hesitancy by some competent authorities and institutions to invest in better financial crime controls. At the same time, risks relating to corruption, tax crime, cash and terrorist financing remain relevant.

6. The TF risks identified in 2021 continue to exist, though the changed geopolitical situation and an increase in right-wing extremism and terrorism have given rise to new TF risks.

7. With few exceptions, awareness of ML/TF risks is increasing across all sectors under the EBA's AML/CFT remit, but the AML/CFT systems and controls institutions have put in place are not always effective. Transaction monitoring and the reporting of suspicious transactions are particularly weak and rated as 'poor' or 'very poor' by between 30% and 50% of competent authorities, with payment institutions and e-money institutions among the worst performing sectors. More competent authorities than ever before have carried out formal ML/TF risk assessments in line with EBA guidelines, and the frequency and intensity of supervisory engagement is increasing, with a tangible impact on levels of inherent and residual risk among credit providers and bureaux de change in particular. Nevertheless, AML/CFT supervision is not always commensurate with perceived levels of ML/TF risk and institutions in some sectors and Member States remain largely unsupervised.

8. In this Opinion, the EBA is issuing 23 proposals to the EU co-legislators and competent authorities to address these risks and to strengthen the EU's financial crime defences.

[2] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 22 January 2020 (EBA/DC/2020/307).

Specific comments

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

10. This Opinion will be published on the EBA's website.

Done at Paris, 13 July 2023

[signed]

José Manuel Campa

Chairperson
For the Board of Supervisors

EBA REPORT

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

EBA/REP/2023/21 July 2023

EBA EUROPEAN BANKING AUTHORITY

Contents

Abbreviations

AMLD	Anti-Money Laundering Directive
AML	anti-money laundering
CA	competent authority
CDD	customer due diligence
CFP	crowdfunding platform
CASP	crypto-assets service provider
CSP	crowdfunding service provider
CFT	countering the financing of terrorism
DORA	Digital Operational Resilience Act
EDD	enhanced due diligence
EMI	e-money institution
ESG	environmental, social and governance
FATF	Financial Action Task Force
FIU	financial intelligence unit
LEA	law enforcement authority
LIU	life insurance undertaking
LII	life insurance intermediarie
MiCAR	Markets in Crypto-Assets Regulation
ML	money laundering
MoU	memorandum of understanding
NCA	national competent authority
NPO	not-for-profit organisation
NRA	national risk assessment
PEP	politically exposed person
RTS	regulatory technical standards

SNRA	supranational risk assessment
STR	suspicious transaction report
TF	terrorist financing
TPA	third-party acquirer
UBO	ultimate beneficial owner

Executive Summary

1. Article 6(5) of Directive (EU) 2015/849 (AMLD4) requires the EBA to issue an Opinion on the ML/TF risks affecting the EU's financial sector every 2 years. 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. This is the EBA's fourth Opinion on ML/TF risks. It is based on data from January 2020 to January 2023, including 49 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. The EBA's Board of Supervisors has approved this Opinion.

3. Since the EBA's third Opinion on ML/TF risks was published in 2021, geopolitical events and technological advances have had a profound impact on the financial sector's exposure to financial crime risks. Russia's invasion of Ukraine in February 2021 led to the imposition by the EU of restrictive measures that are unprecedented in terms of their scale and their scope, but national approaches to enforcing restrictive measures are not harmonised and create pressure on institutions' compliance resources. At the same time, the risk of financial institutions being used to circumvent sanctions has increased. The large-scale displacement of vulnerable persons from Ukraine has led to a surge in human trafficking and given rise to an urgent need to provide access to financial services to refugees from Ukraine. New risks arise from the laundering of proceeds from environmental and cybercrimes, with a perceived increase in risks associated with financial innovation linked to market growth. Legislative developments, including a comprehensive AML Package and the Markets in Crypto-Assets Regulation create legal uncertainty and a hesitancy by some competent authorities and institutions to invest in better financial crime controls. At the same time, risks relating to corruption, tax crime, cash and terrorist financing remain relevant.

4. The TF risks identified in 2021 continue to exist, though the changed geopolitical situation and an increase in right-wing extremism and terrorism have given rise to new TF risks.

5. With few exceptions, awareness of ML/TF risks is increasing across all sectors under the EBA's AML/CFT remit, but the AML/CFT systems and controls institutions have put in place are not always effective. Transaction monitoring and the reporting of suspicious transactions are particularly weak and rated as 'poor' or 'very poor' by between 30% and 50% of competent authorities, with payment institutions and e-money institutions among the worst performing sectors. More competent authorities than ever before have carried out formal ML/TF risk assessments in line with EBA guidelines, and the frequency and intensity of supervisory engagement is increasing, with a tangible impact on levels of inherent and residual risk among credit providers and bureaux de change in particular. Nevertheless, AML/CFT supervision is not

always commensurate with perceived levels of ML/TF risk and institutions in some sectors and Member States remain largely unsupervised.

6. In this Opinion, the EBA is issuing 23 proposals to the EU co-legislators and competent authorities to address these risks and to strengthen the EU's financial crime defences.

1. Background and legal basis

7. The EBA 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, Articles16a(1) and 29(1) (a) of Regulation (EU) No 1093/2010[1], which requires the EBA to issue such an Opinion every 2 years. This Opinion serves to inform competent authorities' application of the risk-based approach to AML/CFT supervision and the European Commission's Supranational Risk Assessment. It is addressed to the European co-legislators and AML/CFT competent authorities.

2. Methodology

8. This Opinion considers ML/TF risks based on data from January 2020 to January 2023 and the following information sources:

- Responses to a questionnaire that was sent to all 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 2020 to December 2021. 49 competent authorities from 29 Member States responded to this questionnaire.

- Submissions to EuReCA, the EBA's AML/CFT database[2].

- Findings from the EBA's reviews of CAs' approaches to AML/CFT supervision.

- Findings from the EBA's work on supervisory colleges.

- Findings from the EBA's peer reviews.

- Findings from the EBA's regulatory and wider risk assessment work, including its work on the scale and impact of de-risking.

- 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 of Regulation (EU) No 1093/2010.

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).

2 EuReCA, the EBA's AML/CFT database

9. As was the case in previous Opinions on ML/TF risks, the EBA analysed this data using a combination of data analytics software and qualitative assessments. The EBA's Board of Supervisors approved this Opinion.

3. Cross-sectoral money laundering and terrorist financing risks

10. **The ML/TF risk landscape has changed**. Since the EBA's Third Opinion on ML/TF risks was published in 2021, geopolitical events, legislative developments and technological advances have had a profound impact on the sector's exposure to financial crime risks and its ability to manage those risks effectively.

11. **Russia's invasion of Ukraine in February 2022 led to the imposition, by the EU, of restrictive measures against Russian and Belarusian interests that are unprecedented in terms of their scale and their scope.** Some financial institutions have responded by shifting resources away from AML/CFT to focus on compliance with these restrictive measures and mitigating circumvention of sanctions. At the same time, legal and regulatory uncertainty has resulted in legitimate customers with links to Russia and Belarus losing access to financial services.

12. **The large-scale displacement of vulnerable persons from Ukraine has led to a surge in human trafficking**. It has also given rise to an urgent need for financial institutions to provide access to financial services to refugees from Ukraine.

13. **The use of complex legal structures to conceal beneficial ownership remains a relevant ML typology**. Its relevance has increased as individuals targeted by restrictive measures seek to conceal their assets. A recent ruling[3], by the European Court of Justice that restricts access to public registries could affect institutions' ability to identify their customers' beneficial owners.

14. **Corruption is a predicate offence to ML and continues to be a central part of the modus operandi of organised crime groups**, as stated in the EU Strategy to tackle Organised Crime 2021-2025[4]. Under the current EU anti-corruption rules, both active and passive corruption of public officials are a crime. The EBA's findings suggest that most CAs are unaware of corruption-related risks, including the risk that institutions in their sector pay bribes to gain or retain business, and they do not consider these risks in their work.

15. **New risks arise from the laundering of proceeds of environmental crimes and cybercrimes**, which are priorities identified as specific predicate offences in the EU Strategy to tackle Organised Crime 2021-2025[5].

16. The Commission published a comprehensive legislative package that, once adopted, will transform the EU's legal and institutional framework. The proposals include a single rulebook

3 Judgment of the Court (Grand Chamber) of 22 November 2022 (requests for a preliminary ruling from the Tribunal d'arrondissement de Luxembourg – Luxembourg) – WM (C-37/20), Sovim SA (C-601/20) v Luxembourg Business Registers

4 EUR-Lex - 52021DC0170 - EN - EUR-Lex (europa.eu)

5 EUR-Lex - 52021DC0170 - EN - EUR-Lex (europa.eu)

on AML/CFT and the establishment of a central EU AML/CFT Authority (AMLA) with direct supervisory powers. They address many of the challenges the EBA had highlighted in its 2020 Response to the Commission's Call for Advice on the Future AML/CFT Framework. At the same time, ongoing negotiations of the AML/CFT package and the scale of the proposed reforms have created legal uncertainty and a reluctance by some competent authorities and institutions to proceed with investments in their financial crime controls.

17. Financial innovation continues apace and creates significant opportunities for the adoption by institutions and their supervisors of more effective AML/CFT controls. New technology that is ill applied or understood also carries financial crime risks. DORA might reduce some of the associated risks with regard to FinTech, BigTech and RegTech.

18. The AML/CFT package along with the MiCAR will introduce a wider range of crypto-assets within the EU regulatory perimeter and subject them to AML/CFT requirements.

Scanning the horizon: the digital euro

In October 2020, the Eurosystem published a report on a digital euro[6], following a decision by the ECB's Governing Council to advance work on the possible issuance of a digital euro. If adopted, the digital euro would consist of an electronic form of central bank money accessible to all EU citizens and firms. It would be introduced alongside cash, without replacing it.

In April 2023, the Eurosystem published its third report on the investigation phase of the digital euro[7], which aims to address key issues relating to the design and distribution of a digital euro. In light of the EC legislative proposal on a regulation to establish a digital euro[8], two foundational design options are still being discussed, among others: peer-to-peer validated offline transactions (i.e. similar to cash), and third-party validated online transactions (i.e. similar to digital payments).

As the digital euro will be distributed by regulated intermediaries, including credit institutions, payment institutions and e-money institutions, any vulnerabilities associated with these intermediaries' AML/CFT controls will also affect the digital euro. The EBA's findings in Sections 4.1, 4.2 and 4.3 of this report suggest that these risks could be significant. ML/TF risks could arise inter alia from vulnerabilities associated with the imprudent and inadequate use of remote customer onboarding processes, insufficient oversight of outsourcing arrangements, if any, the possibility to undertake proximity offline payments, including via prepaid cards, funding and defunding digital euro accounts with cash, and the anonymity of transactions below a certain threshold.

The possible lack of coordination between AML/CFT supervisors of those intermediaries, which is highlighted in Section 3.3.3 of this report, could further affect the effectiveness of the EU's AML/CFT framework in this regard.

6 European Central Bank Eurosystem, Report on a digital euro

7 European Central Bank, Eurosystem, Progress on the investigation phase of a digital euro – third report

8 Digital euro package

3.1 Cross-sectoral risks that are new or emerging

19. The EBA has identified new risks or risks arising from specific contexts that were not identified in the 2021 Opinion. These include the implementation of restrictive measures, human trafficking, identification of ultimate beneficial ownership, identification of politically exposed persons, vulnerabilities in qualifying holdings, laundering of proceeds of environmental crimes and cybercrime.

3.1.1 National approaches to enforcing compliance with restrictive measures are not harmonised

20. Since Russia's annexation of Crimea in 2014, the EU has imposed sanctions on 1 800 individuals and entities as of June 2023. These measures are unprecedented in their scale and scope and have highlighted that Member States' approaches to interpreting and enforcing them diverge. This creates significant compliance challenges for financial institutions and weakens the impact of the EU's regime.

21. There are marked differences in the way Member States organise the supervision of financial institutions in this regard. Uneven approaches relate to the powers supervisors have, with responsibilities for testing the adequacy of systems and controls allocated to different types of supervisors, including AML/CFT supervisors, prudential supervisors and the national competent authority for the enforcement of restrictive measures, shared between multiple domestic authorities or assumed by none at all. Uneven approaches also relate to the expectations different authorities have of institutions' sanctions systems and controls. By 2020, most CAs responsible for supervising institutions' restrictive measures systems and controls had not assessed compliance of their sector. By 2022, in the wake of sanctions against Russia and Belarus, thematic reviews were underway in several Member States but in other Member States, institutions' sanctions systems and controls were not supervised at all. Not all CAs had issued guidance to their sector on the systems and controls to be implemented for compliance, with several CAs indicating that they did not have the legal basis to do so.

22. Feedback from institutions confirms the EBA's findings that uneven approaches to the supervision of institutions' sanctions systems and controls can make compliance difficult. For example, during implementation reviews, private sector representatives indicated to the EBA's review teams that they had been supervised by three different competent authorities that each took a different view on the adequacy of the same sanctions policies and procedures, and the manner key sanctions provisions should be interpreted. These issues were further exacerbated where institutions operated on a cross-border basis. From the onset of the Russian aggression against Ukraine, the EBA has proactively facilitated information sharing in

colleges on the (direct and indirect) implications on the banking groups and its subsidiaries/branches and for coordinating supervisory actions[9].

23. The Regulation (EU) 2023/1113 introduces a mandate for the EBA to issue guidelines on 'internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures when performing transfers of funds and crypto-assets under this regulation'[10]. These guidelines will clarify supervisory responsibilities and foster a common understanding by competent authorities and financial institutions of the policies, procedures and controls that are necessary to comply effectively with restrictive measures regimes. The EBA will consult on these guidelines once the Regulation has been published.

3.1.2 Non-compliance with restrictive measures gives rise to operational and legal risks for financial institutions and can lead to unwarranted de-risking

24. CAs that have the legal power to assess the adequacy of their sector's sanctions systems and controls indicated that they do so before granting authorisations, through dedicated questions in the annual AML/CFT questionnaire, thematic reviews or as part of full-scope AML/CFT on-site inspections. The intensity and intrusiveness of these assessments varied in line with the chosen supervisory tools.

25. CAs that responded to the questionnaire and had taken supervisory action indicated that the most common shortcomings they had identified related to a lack of understanding by financial institutions of their exposure to sanctions risks. The lack of internal policies and procedures was noted, such as absent procedures for sanctions alerts processing, record keeping and assets freezing and where they existed, internal controls were not always sufficient to ensure the effective application of those policies and procedures by employees.

26. Deficiencies in screening systems were common, with institutions using outdated or incorrect sanctions lists and relying unquestioningly on vendors' screening systems. Screening systems were not always adequately calibrated and their scope was at times narrowly set. This meant that institutions failed to screen high-risk customers or transactions, which exposed them to significant legal risks.

27. Finally, CAs highlighted that to be effective, policies and procedures to comply with restrictive measures must be built on effective due diligence measures. Poor AML controls with incomplete, inaccurate or outdated CDD and EDD information may not allow institutions to identify sanctions targets or suspicious changes in shareholding structures, which can be used to obfuscate beneficial ownership.

28. Inadequate sanctions systems and controls do not only expose the sector to legal risks, but also lead to the unwarranted de-risking of legitimate customers. Evidence from competent

9 Report on convergence of supervisory practices in 2022 – EBA/REP/2023/11

10 Article 23 at eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2023:150:FULL

authorities and financial sector representatives suggests that through 2022, this was the case for Ukrainian refugees and customers with links to Russia or Belarus that are legally resident in the EU.

Box 1. EBA statement on financial inclusion in the context of the invasion of Ukraine

In April 2022, the EBA published a statement[11] setting out what financial institutions and their supervisors can do to provide access to refugees from Ukraine to the EU's financial system. The EBA also set out what financial institutions and supervisors can do to protect vulnerable persons from abuse by criminals, to prevent human trafficking (see more in Section 3.1.3) and called on financial institutions to ensure that compliance with the EU's restrictive measures regime does not lead to unwarranted de-risking.

3.1.3 Efforts to tackle human trafficking through financial inclusion are disjointed and often inadequate

29. Following the invasion of Ukraine in 2022, millions of people have found refuge in EU Member States. All refugees are vulnerable and may be at significant risk of human trafficking and exploitation[12].

30. Five CAs prepared a circular on risks associated with human trafficking, and 6 CAs organised roundtables and training events for their supervised sector, like a public-private forum. But 74% of CAs that responded to the questionnaire indicated that no authority in their jurisdiction had assessed risks arising from the laundering of proceeds of human trafficking. When such an assessment was made by another authority, for example the FIU, law enforcement or in the national risk assessment, 26% of CAs did not use such an assessment to set supervisory expectations of financial institutions within their supervisory remit.

31. Handling the proceeds from human trafficking and exploitation is a crime. Information exchange on risk indicators associated with human trafficking between competent authorities, financial institutions, FIUs and LEAs can help raise awareness of the ML/TF risks associated with human trafficking and exploitation, and to improve steps financial institutions can take to detect and report it to their local FIU without delay.

32. These risks of human trafficking can be reduced by providing refugees with access to financial services[13]. The EBA's guidelines on policies and controls for the effective management of ML/TF risks when providing access to financial services[14], which were published in March 2023,

11 EBA statement on financial inclusion in the context of the invasion of Ukraine

12 Early_Warning_Notification__War_in_Ukraine_–_refugees_arriving_to_the_EU_from_Ukraine_at_risk_of_exploitation_as_part_of_THB.pdf (europa.eu)

13 FAST, Finance against Slavery and Trafficking

14 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

set out steps for financial institutions to consider before making a decision about customers. Several options need to be considered, as explained in Box 8 of Section 3.2.8.

Proposal: The EBA advises CAs to take the steps necessary to understand their sector's exposure to the risk that institutions may be handling the proceeds from human trafficking and take steps commensurate with that risk to mitigate it.

3.1.4 Deficiencies in the identification of ultimate beneficial ownership undermine the effectiveness of the Union's AML/CFT and restrictive measures regimes

33. The use of complex legal structures, with stacking of companies and front persons, to conceal the UBO is a feature of most large-scale cases of money laundering. This typology is also relevant in other cases, including the concealment of assets of an individual person targeted by restrictive measures and in tax-avoidance schemes such as those highlighted in the Pandora Papers and Paradise Papers. Eurojust identified[15] several complex money laundering cases illustrating challenges associated with the establishment of beneficial ownership.

34. The majority of CAs indicated that they provide guidance to institutions on the identification of beneficial owners through information letters, circulars, training and guidelines. Supervisory activities range from dedicated questions in annual AML/CFT questionnaires, to off-site reviews, thematic review and targeted inspections. CAs assess the adequacy and effectiveness of institutions' controls to identify and verify UBOs.

35. CAs indicated that 38% of financial institutions from all sectors have a 'moderately significant' exposure to UBOs from other EU/EEA jurisdictions. The exposure of the EU financial sector to complex corporate structures is considered by CAs to be 'moderately significant' to 'significant'. Inspection findings suggest that EU financial institutions are not well equipped to mitigate those risks, as CAs consider that 26% of financial institutions across all sectors lack adequate systems and controls to identify UBOs.

Box 2. The ML/TF Risk Factors Guidelines[16]

In 2021, based on findings from previous Opinions on ML/TF risk, the EBA updated its ML/TF Risk Factors Guidelines to include provisions on the identification and verification of customers' beneficial owners. Guidelines 4.12 to 4.25 focus on the use of beneficial ownership registers, control through other means, identifying the customer's senior managing officials and identifying the beneficial owner of a public administration or a state-owned enterprise.

15 Eurojust, Report on money laundering

16 Guidelines 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/2021/02

The Guidelines also set clear expectations of financial institutions' AML/CFT systems and controls in relation to risks associated with jurisdictions that are associated with high levels of predicate ML/TF offences, including corruption.

36. Several CAs indicated that setting up the domestic beneficial owner register has significantly increased transparency of the beneficial ownership of legal entities.

37. In 2022, a ruling[17] by the European Court of Justice invalidated a 2018 amendment to the AMLD, which had granted the general public access to EU countries' beneficial ownership registries. This might limit the ability of financial institutions in certain Member States to retrieve information on UBOs. It could also have an adverse impact on the quality and accuracy of the information contained in these registries as limiting public access reduces opportunities for review and feedback. In 2023, the European Data Protection Board letter[18] on data sharing for AML/CFT purposes suggests further limiting public access provisions in the future AML/CFT package to safeguard fundamental rights to privacy and protection of personal data.

3.1.5 PEPs identification measures remain an important component of the fight against corruption

38. Under the current EU anti-corruption rules, Member States are required to criminalise both active and passive corruption of public officials, establish adequate sanctions and ensure that entrepreneurs corrupting officials are held criminally liable. Article 20 of Directive (EU) 2015/849 requires financial institutions to take risk-sensitive steps to establish whether their customer, or their customer's beneficial owner, is a PEP and if they are a PEP, apply EDD measures to mitigate the risk that they may be used to launder the proceeds from corruption.

39. Based on their supervisory work, most CAs considered that their sector's exposure to ML/TF risks associated with PEPs was 'not significant' but a quarter of CAs that responded to the questionnaire had not taken any formal steps to assess these risks. In addition, most CAs indicated that they do not consider other corruption-related risks, including the risk that institutions in their sector pay bribes to gain or retain business.

40. Those findings raise concerns about the role supervisors play in the fight against corruption.

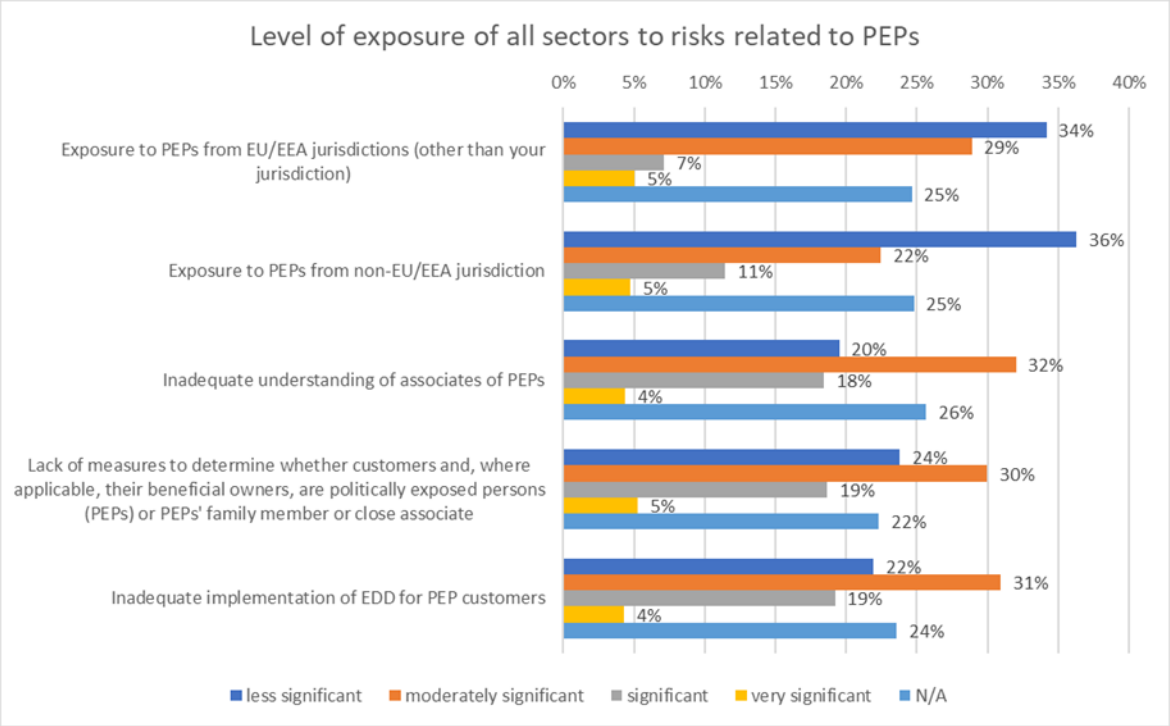
41. The Commission announced new initiatives to fight corruption in the 2022 State of the Union Address and in May 2023 published an anti-corruption package[19] comprising a Communication on an EU anti-corruption policy, a proposal for a directive based on Article 83(1) TFEU and a dedicated Common Foreign and Security Policy sanctions regime to target serious acts of corruption worldwide.

17 Judgment of the Court (Grand Chamber) of 22 November 2022 (requests for a preliminary ruling from the Tribunal d'arrondissement de Luxembourg – Luxembourg) – WM (C-37/20), Sovim SA (C-601/20) v Luxembourg Business Registers

18 EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML-CFT purposes in light of the Council's mandate for negotiations

19 Anti-corruption: Stronger rules to fight corruption in the EU and worldwide

Figure 1: Level of exposure of all sectors to risks related to PEPs



Box 3. EBA report[20] on competent authorities' response to the 2020 Luanda Leaks

The EBA worked to understand the steps AML/CFT competent authorities in the EU had taken to assess the ML/TF risks to which their sector was exposed, in light of the information contained in the documents leaked by the International Consortium of Investigative Journalists (ICIJ). The EBA found that competent authorities across the EU adopted significantly different approaches for identifying and tackling money laundering (ML) and terrorist financing (TF) risks highlighted by the leaks. These approaches varied beyond what the EBA would have expected under a risk-based approach. This suggests that there is a risk that proceeds from corruption may not be detected and may be laundered through the EU's financial sector.

Proposal: The EBA advises CAs to take the steps necessary to understand the risk that institutions in their sector launder the proceeds from corruption or act corruptly themselves.

3.1.6 Competent authorities need to reach out to prudential supervisors in charge of ESG and environmental agencies to strengthen the fight against laundering of proceeds of environmental crime

20 Report on competent authorities' response to the 2020 Luanda Leaks - EBA/REP/2022/05

42. Environmental crime, including illegal waste trafficking, illegal trade with endangered species, illegal gold mining and the violation of environmental regulation, is a predicate offence to ML and highlighted in the EU Strategy to tackle Organised Crime 2021-2025. Both the FATF[21] and Eurojust[22] have assessed that environmental crime is one of the most profitable criminal enterprises.

43. 83% of CAs responding to the questionnaire indicated that no authority in their jurisdiction assessed risks arising from the laundering of proceeds of environmental crimes. When such an assessment was made by another authority, most of the time the FIU, the LEA or an environmental protection agency, half of CAs did not use this risk assessment to assess their sector's exposure, but 2 CAs prepared a circular on risks associated with environmental crime, and 3 CAs organised roundtables and training events for their supervised sector, like public-private fora.

Proposal: The EBA advises CAs to take the steps necessary to understand the risk that institutions in their sector might be laundering the proceeds from environmental crime.

3.1.7 AML/CFT authorities have a limited awareness of risks associated with laundering the proceeds from cybercrime

44. Cybercrime[23], including phishing/vishing, ransomware, CEO fraud, cyber-attacks of financial institutions, misuse of payment cards, blackmailing, love scams, drugs and weapons trafficking on the darknet, is a predicate offence to ML.

45. 70% of CA responding to the questionnaire indicated that no authority in their jurisdiction assessed risks arising from the laundering of proceeds of cybercrimes. When such an assessment was made by another authority, approximately one third of CAs did not use this assessment to assess the risk exposure of their supervised financial institutions and manage identified risks. Five authorities prepared a circular on risks associated with cybercrimes, and 7 CAs organised roundtables and training events for their supervised sector, like public-private fora.

46. CAs considered that sectors that are particularly vulnerable to the laundering of proceeds of cybercrime are credit institutions, payment institutions, and crypto-assets service providers.

Proposal: The EBA advises CAs to take the steps necessary to understand their sector's exposure to the risk that they may be used to launder the proceeds from cybercrime.

21 Money Laundering from Environmental Crime (fatf-gafi.org)

22 Report on Eurojust's casework on environmental crime

23 Europol, Internet Organised Crime Threat Assessment

Box 4. DORA and cybersecurity

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) ensures convergence and harmonisation of security and resilience practices across the EU. DORA aims to establish a regulatory framework for the oversight of critical ICT third-party providers, including rules for ICT risk management, ICT incident reporting, digital operational resilience testing and third-party risk management. DORA will apply from 17 January 2025.

The ESAs (EBA, ESMA and EIOPA) will develop a total of 12 joint policy mandates, a feasibility report on a single EU Hub for incident reporting along with the implementation of the ESRB recommendation and the Call for Advice from the European Commission on DORA delegate acts.

The following policy work has to be developed in cooperation with the ENISA, the EU agency for cybersecurity:

-RTS on ICT risk management framework (Art. 15);

-RTS on simplified ICT risk management framework (Art. 16);

-RTS on criteria for the classification of ICT-related incidents (Art. 18.3);

-RTS on specifying the reporting of major ICT-related incidents (Art. 20.a);

-Implementing Technical Standards to establish the reporting details for major ICT-related incidents (Art. 20.b);

-Guidelines on the estimation of aggregated annual costs/losses caused by major ICT incidents (Art. 11.12);

-Feasibility report for establishing a single EU Hub for major ICT-related events (Art. 21).

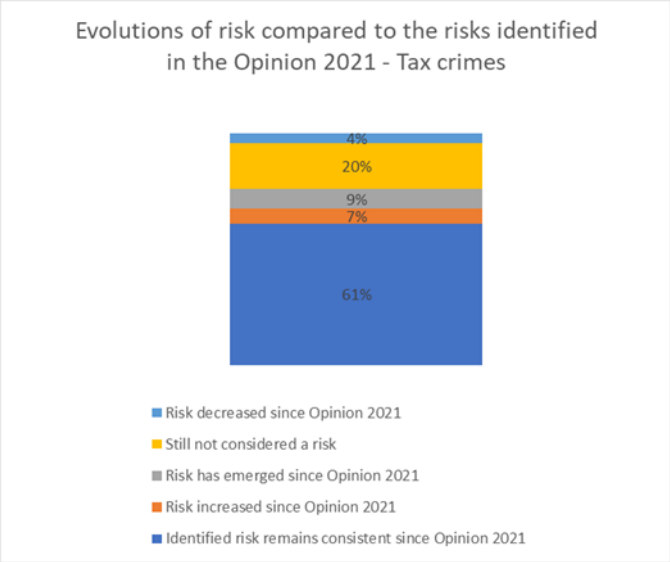
3.2 Existing risks that remain relevant

47. In the 2021 Opinion on ML/TF risks, the EBA identified a number of risks that were cutting across different sectors. These include risks associated with tax-related crimes, crypto-assets, FinTech activities, RegTech solutions, the COVID-19 pandemic, and de-risking. Most of these risks remain relevant.

3.2.1 AML/CFT supervisors and tax authorities need to cooperate more in the fight against tax crimes

48. For most CAs, the risks related to the laundering of proceeds from tax crimes, such as tax evasion and tax fraud have remained constant since the 2021 Opinion was published.

Figure 2: Evolution of risks in relation to tax crimes



49. Three CAs indicated that risks had increased. In two cases, this was because of an increase in tax crimes during the COVID-19 pandemic, specifically VAT fraud and social benefit fraud. In one case the assessment had changed because the CA's understanding of these risks had improved based on updates to their Member States' NRA.

50. Four CAs indicated that laundering the proceeds from tax crimes had taken on a new significance in their Member State. In some Member States, this was triggered by a sudden increase in the proportion of STRs linked to tax crimes. In other Member States, tax-related crimes had only recently been designated as predicate offences for ML.

51. Two CAs indicated that this risk had decreased. They said this was due to the improved implementation of international tax transparency agreements, including Common Reporting Standard and Foreign Account Tax Compliance Act.

52. Nine CAs believe that tax-related crimes are not relevant. They explained that tax crime is not a predicate offence to ML in their Member State and that they were not competent to take action in this regard. Consequently, they did not cooperate with national tax authorities.

53. Several CAs had taken steps to raise awareness of ML/TF risks arising from tax-related crimes and possible ways to mitigate these risks. For example, one CA requested institutions providing asset management activities or issuing single-premium life insurance policies to carry out a dedicated internal tax crimes audit. Others issued circulars to remind institutions that facilitating tax evasion was a crime. Nevertheless, supervisory findings suggested that awareness among some financial institutions remained limited. Furthermore, EBA findings from its ongoing programme of reviews of competent authorities' approaches to tackling ML/TF risk in banks suggested that in several Member States, tax crimes had been identified as a major ML risk in the NRA, but that this had not been reflected in supervisors' own risk assessments or action plans. This meant that in those Member States, in the absence of

sufficient interest from supervisors, institutions did not focus on tackling the laundering of proceeds from such crimes.

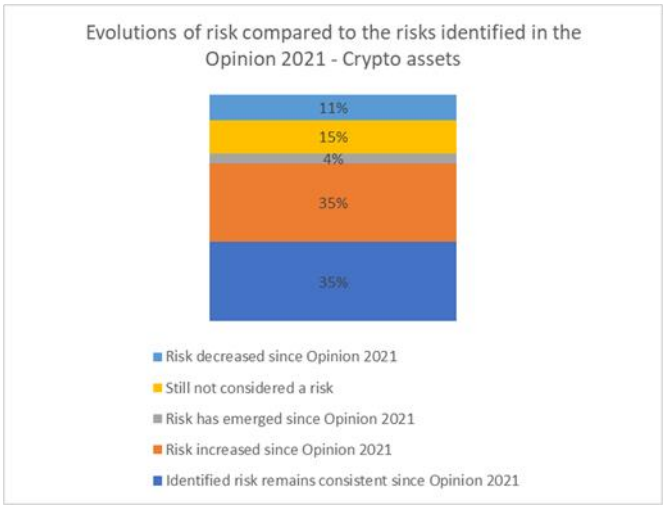
54. Through 2021, the EBA continued to implement the 10-point CumEx Action Plan[24] that it had adopted in 2020. By the end of 2022, 9 out of 10 action points had been completed, with the remaining action point, an inquiry into the actions taken by financial institutions and national authorities to supervise compliance with requirements applicable to dividend arbitrage trading schemes, due to be carried out in 2023.

Proposal: The EBA advises CAs take the steps necessary to understand the risk that institutions in their sector might be facilitating or laundering the proceeds from tax crimes.

3.2.2 Risks related to crypto remain but change is underway

55. The 2021 Opinion highlighted that most CAs assessed crypto-assets as presenting significant ML/TF risks. An important factor at the time was the growth of the crypto-assets market, in terms of transactions processed and number of firms' clients that use crypto-assets or are considered obliged entities in the Member States. CAs also pointed to the opacity of transactions and identities of end customers involved in crypto-assets activities that in the context of several typologies, may facilitate illegal activities.

Figure 3: Evolution of risks in relation to crypto-assets



56. In their responses to the 2023 EBA's questionnaire, a third of CAs indicated that ML/TF risks from crypto-assets have increased further since the last Opinion was published in 2021. This was because of continuous growth of the crypto-assets market within recent years and, the incremental awareness of the risks associated with the novel crypto-related business models (including the use of technology designed to prevent transparency, such as tumbling or mixing

24 EBA Action plan on dividend arbitrage trading schemes ('Cum-Ex/Cum-Cum')

services or anonymity-enhanced coins) by the EU Members States as consequence of the recent regulatory agendas. Consequently, CAs have started factoring crypto-assets within the scope of their supervisory programmes (for instance, AML/CFT national risk assessments, inspections, etc.) concluding that the risks associated with crypto-assets are relatively high or have grown over recent years (see more in Section 4.11) and have been intensified by the fact that they are not yet widely captured by the existing regulatory frameworks.

57. CAs that consider that risks have decreased since the last Opinion noted that inherent risks remain high, but that they were effectively managed. They were confident that their AML/CFT work had improved CASPs' ML/TF risk management capabilities. For example, some CAs explained that changes in domestic regulation removed riskier products, which have moved outside of the EU. Others highlighted that CASPs' risk appetite had decreased.

58. Competent authorities' perceptions and assessments of crypto-assets risks are directly related to the current legal framework.

- First, the 5th AML Directive (AMLD5) brought custodian wallet providers and providers engaged in exchange services between virtual and fiat currencies within the scope of the AML/CFT legal framework by defining them as obliged entities. Member States had to transpose the AMLD5's provisions into their national laws by 10 January 2020. The AMLD5 is a minimum-harmonisation Directive, which means that Member States are allowed to go beyond the minimum standard set by the Directive when transposing it into national law. The legal requirements that apply to custodian wallet providers and providers engaged in exchange services between virtual and fiat currencies and competent authorities' approaches to the AML/CFT supervision of those entities therefore vary depending on each country's legal framework, and their approach to supervision. For example, virtual currency exchange platforms (VCEPs) and custodian wallet providers (CWPs) are not always supervised by the competent authority that is responsible for the AML/CFT supervision of credit and financial institutions, which can hamper information exchange between competent authorities in different Member States. This lack of a consistent approaches to AML regulation and supervision stood until the MiCAR Regulation entered into force.

- Second, although crypto-assets have existed for roughly a decade, they have remained largely unregulated and unsupervised and thus, providers are less mature in terms of their compliance efforts than other obliged entities under the AMLD. This is apparent from recent enforcement cases in the EU.

59. Now published, the MiCAR has the effect of expanding the EU regulatory perimeter to a wider range of crypto-asset activities to help regulate currently out-of-scope crypto-assets and their service providers in the EU. This is the first step, alongside the Regulation (EU) 2023/113 on information accompanying transfers of funds and certain crypto-assets, from a legislative point of view to a harmonised approach to crypto-assets and will boost the development of a convergent approach to the supervision of crypto-assets activities and robust cross-sectoral cooperation on AML/CFT matters.

Box 5. New EBA mandates under TFR and MiCAR

Regulation (EU) 2023/113 on information accompanying transfers of funds and certain crypto-assets intends to bring the EU's legal framework in line with the FATF standards by extending the obligation to include information about the originator and beneficiary to CASPs – the travel rule. As per the mandates provided in this Regulation, the EBA is:

-extending the ESA's 2017 TFR Guidelines to crypto-asset service providers;

-extending the existing EBA's ML/TF Risk Factors Guidelines[25] and the EBA's Risk Based AML/CFT Supervision Guidelines to crypto-asset service providers[26];

The MiCAR provides a new supervisory role to the EBA and a number of mandates to deliver regulatory products.

3.2.3 An increase in risks associated with FinTech may be linked to the booming market

60. Most CAs consider that ML/TF risks associated with FinTech activities affects all sectors with the exception of bureaux de change and remains the same as in 2019/2020, but almost a quarter of CAs indicated that risks had increased or emerged. Where this was the case, this appeared to be linked to increased market shares with a digital acceleration[27], rather than a change in inherent risks, which have remained largely unchanged.

25 Consultation paper on 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/CP/2023/11

26 Consultation paper on Guidelines amending Guidelines EBA/GL/2021/16 on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (The Risk-Based Supervision Guidelines) - EBA/CP/2023/05

27 Report on the use of Digital platforms in the EU banking and payments sector - EBA/REP/2021/26

Figure 4: Evolution of risks in relation to FinTech

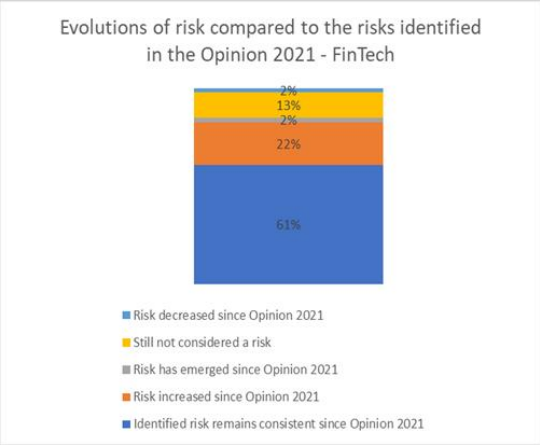
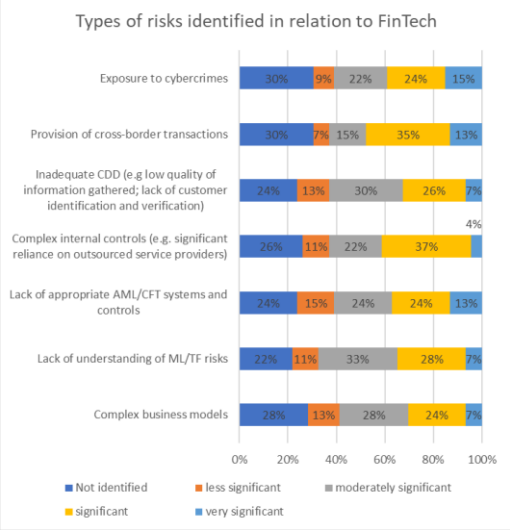


Figure 5: Types of risks identified in relation to FinTech



61. Most CAs identified the lack of understanding by FinTech providers of ML/TF risks as posing a moderate to significant risk. Assessments of risk in relation to the adequacy of AML/CFT systems and controls varied, with many CAs considering this a very significant risk, and others considering the risk to be moderately significant to significant. Over-reliance on outsourced service providers without appropriate safeguards is a significant risk in the view of most CAs.

62. More specifically, CAs noted that the increasing number of Fintech applications as providers to credit institutions' customers provides greater opacity of the transactions and a decrease in their traceability. The importance of payment initiation service providers (PISPs) and account information service providers (AISPs) in the provision of innovative and fully digital payment services is expected to increase as the transition to open banking intensifies.

63. Technical solutions enable complex product offerings, including an increase in complexity. The risk is that high-risk products are offered to a greater extent and that the efficiency of KYC and transaction monitoring may suffer. Oversight by firms and competent authorities require technology changes to be robust, operate as designed and in compliance with legislation.

Box 6. EBA Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

In those Guidelines[28], the EBA establishes common EU standards on the development and implementation of sound, risk-sensitive initial customer due diligence policies and processes in the remote customer onboarding context. They set out the steps financial institutions should take when choosing remote customer onboarding tools and when assessing the adequacy and reliability of such tools, in order to comply effectively with their AML/CFT obligations. The Guidelines are technologically neutral and do not prioritise the use of one tool over another.

3.2.4 BigTech firms can provide financial services but are not always subject to AML/CFT rules or supervision

64. BigTech refers to large technology companies with extensive customer networks. It includes firms with core businesses in social media, internet search, software, online retail and telecoms. BigTechs are facilitating the provision of financial services by financial institutions, for example via a payment platform and cloud service provision and some are providing financial services directly in parallel to other business lines. Only a limited number of BigTech group companies currently have subsidiaries holding licences to carry out financial services activities in the EU, with eight known to have subsidiary companies carrying out regulated financial services[29]. Each of these is carrying out its regulated services across a number of EU Member States as a result of 'passporting' arrangements. The ESAs also observe[30] growing interactions between incumbent financial institutions, FinTechs and BigTechs through a variety of co-operation models, e.g. partnerships, joint ventures, outsourcing and sub-outsourcing, mergers and acquisitions.

65. BigTech are 'mixed activity groups', i.e. parent undertakings and its subsidiary undertakings conducting both financial and non-financial services. This raises some challenges for the AML/CFT framework. Although licensed subsidiaries established in Europe are subject to the AML/CFT requirements, other operating subsidiaries of these tech giants, particularly those dedicated to e-commerce, are purely commercial undertakings and are not subject to banking or AML/CFT regulations. 9% of the CAs (4 CAs) who responded to the questionnaire indicated they identified ML/TF risks in relation to BigTech, whether through direct supervision or in the context of supervision of other financial institutions. Key risks identified are lack of appropriate AML/CFT systems and controls, over-reliance on third parties for CDD purposes, provision of cross-border transactions, exposure to cybercrimes and functions in facilitating the fragmentation of value chains[31].

28 Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849 - EBA/GL/2022/15

29 Joint ESA response to the EC's February 2021 call for advice on digital finance – ESA 2022 01

30 ESA 2022 01

31 Report on the use of Digital Platforms in the EU banking and payment sectors – EBA/REP/2021/26

Proposal: The EBA advises EU co-legislators to consider including financial services provided by mixed activity groups as obliged entities under the AML/CFT framework.

Box 7. DORA and BigTech

The new EU legislation on digital operational resilience (DORA), which entered into force on 16 January 2023 which will apply from 17 January 2025, will establish *inter alia* an EU oversight framework applicable to all critical ICT third-party service providers, which provide ICT services to EU financial entities. It could be possible that some BigTech companies that offer ICT services to EU financial entities might fall under the upcoming EU oversight framework if they are designated as critical. This will allow for a continuous monitoring of the activities of the critical ICT third-party service providers to financial entities. In the context of the oversight framework, a lead overseer (one of the ESAs) will be appointed for each critical ICT third-party service provider and it will pay particular attention to fully grasp the magnitude of interdependences, discover specific instances where a high degree of concentration of critical ICT third-party service providers in the EU is likely to put a strain on the financial system's stability and integrity and maintain a dialogue with critical ICT third-party service providers where that specific risk is identified. The lead overseers will be able to effectively conduct monitoring missions and inspections to assess the rules, controls and processes used by the critical ICT third-party service providers, as well as assess the potential cumulative impact of their activities on financial stability and the integrity of the financial system, resulting in recommendations addressed to these providers.

3.2.5 Risks associated with the use of RegTech solutions are perceived to have increased

66. In the 2021 Opinion, most CAs did not consider the use of RegTech solutions by obliged entities as a risk. This proportion has changed, with several new CAs now identifying this risk, and 9% indicating that the risk has increased. This is similar to the findings in the EBA Analysis of RegTech in the EU financial sector[32]. All sectors are identified as vulnerable to risks associated with the use of RegTech solutions, except bureaux de change.

67. As regards the types of risks associated with the use of RegTech solutions, CAs highlighted ML/TF risks related to IT reliability, potentially leading to fraud risks, as the most relevant (30% of CAs consider it as posing a significant or very significant risk). Lack of internal skills and experience in financial institutions to develop or adopt RegTech solution poses a moderately significant risk. The interpretation of data protection rules can limit effective information sharing and can pose a 'significant' to 'very significant' risk as well. Faulty solutions potentially leading to fraud risks was assessed as 'less significant' to 'moderate' risk. CAs indicated that a 'less significant' to 'moderately significant' concentration risk exists when a few RegTech solutions are adopted by the majority of supervised entities.

32 EBA Analysis of RegTech in the EU financial sector – EBA/REP/2021/17

68. The growing use of RegTech solutions by financial institutions might expose them to outsourcing risks because of over reliance on third party service providers and increased reliance on CDD controls carried out by other financial sector entities without sufficient controls in place. Moreover, CAs indicated the emergence of artificial intelligence and machine learning solutions has been increasing automation, enhancing efficiencies, consistency and quality of processes, but can nevertheless create transparency challenges of the transaction monitoring system outputs and, in the worst case, result in the creation of a black box for the end user. It is, therefore, crucial that when such systems are used the model risk is appropriately managed over time. If such classic tools with a pre-defined set of scenarios and rules were to be replaced by complex algorithms and big data-driven tools, supervisors should ensure that this does not come at the expense of the transparency and explainability of the transaction monitoring system. When such systems are used, the model risk needs to be appropriately managed by financial institutions.

Figure 6: Evolution of risks in relation to RegTech

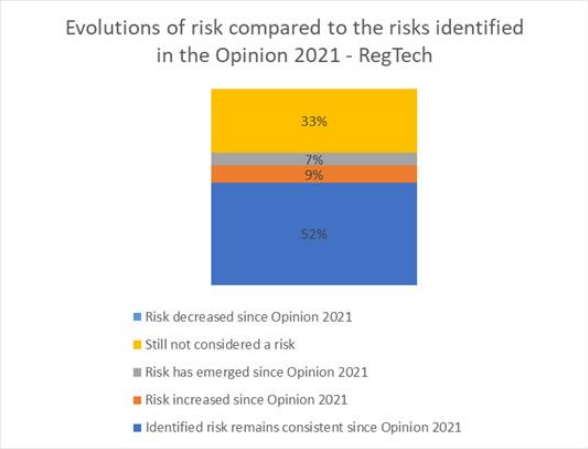
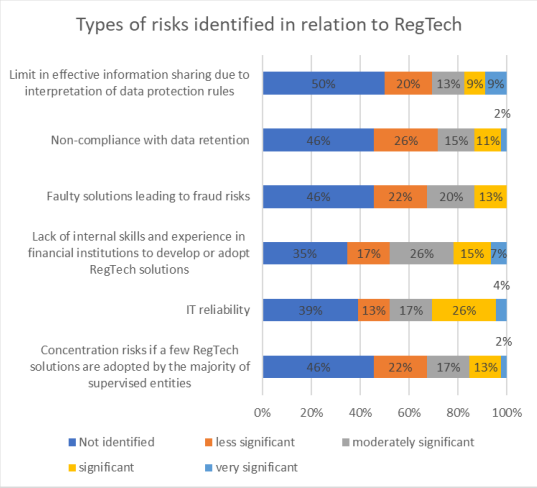


Figure 7: Types of risks identified in relation to RegTech



3.2.6 Questions remain over the effectiveness of the fight against terrorist financing

69. The responses received through the EBA questionnaire indicate that for almost all CAs, the risks identified in 2021 remain constant and that the observations set out in the 2021 Opinion remain relevant. Only 3 CAs considered that the risk had increased, and where this was the case, this was due to a change in the geopolitical situation, or an increase in right-wing

extremism and terrorism. Europol's annual EU Terrorism Situation and Trend Report[33] (TE-SAT) concurs with those findings.

70. On the contrary, 3 CAs considered that terrorist financing risks had decreased. They suggested that this was due to better awareness of the supervised sector through supervision, a change in customer portfolios or the domestic security policy.

71. CAs identified TF risks in almost all sectors, but the risks appear to be particularly relevant to sectors associated with the use of cash, occasional transactions and high-risk jurisdictions such as payment institutions, bureaux de change, e-money institutions, crypto-assets service providers and credit providers (other than credit institutions).

72. CAs were concerned that TF risks were insufficiently managed across all sectors, with systems and controls deficiencies linked to a lack of understanding of terrorist financing risks, and an over-reliance on screening targeted financial sanctions lists as the only monitoring tool.

Figure 8: Evolution of risks in relation to terrorist financing

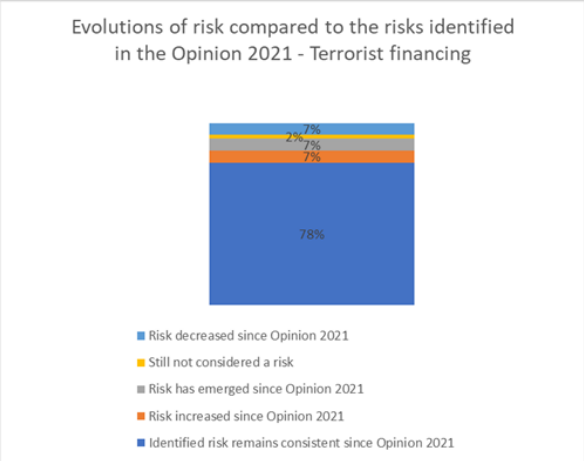
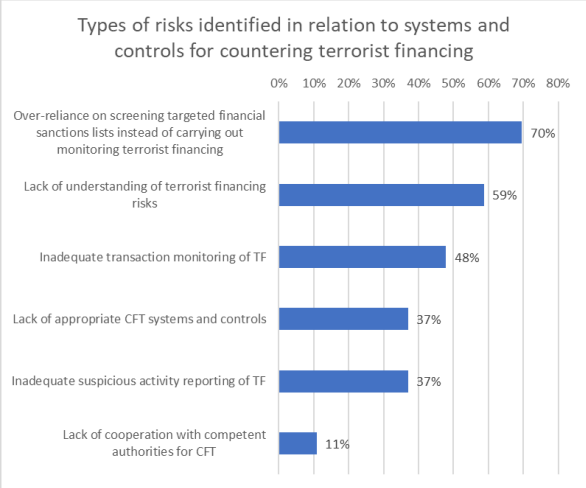


Figure 9: Types of risks identified in relation to systems and controls for CFT



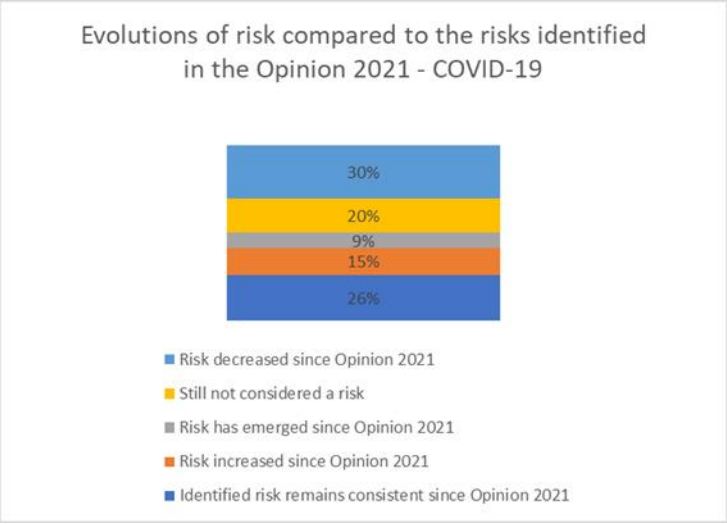
33 Europol's annual EU Terrorism Situation and Trend Report

73. At the same time, findings from the EBA's implementation reviews suggest that not all CAs are equipped effectively to assess and mitigate TF risks in their sector, as most competent authorities' understanding of TF risk remains limited. For example, some competent authorities appeared to be unaware of TF risks arising from right-wing extremism, which law enforcement in these Member States had highlighted to the review team as an area of growing or significant concern. Some competent authorities did not consider that the risk of TF had increased in their sector despite it servicing a significant number of customers with links to countries and territories with a high TF risk, which meant that cross-border transfers of funds to the countries and territories in these sectors were prevalent.

3.2.7 Risks linked to the COVID-19 pandemic are decreasing but new approaches to AML/CFT supervision remain

74. Views of CAs appear to diverge on the continued relevance of risks related to the COVID-19 pandemic, with 30% considering that the risk has decreased, 26% considering that the risk remained consistent, and 24% considering that it has emerged or increased. 20% of CAs did not identify any risks. A possible explanation might be that the questionnaire was referring to data from 2020 and 2021, but that some CAs assessed the risk at as of 2022, which led to a perception of decreasing risks.

Figure 10: Evolution of risks in relation to COVID-19



75. Most CAs indicated that remote client onboarding was widespread during the pandemic. This created risks at the beginning of the pandemic as some financial institutions had to adapt quickly to remote onboarding, which was not a common practice in their Member States. CAs consider that they helped supervised entities to adapt, and that as a result, the use of solution for remote clients identification of the customers and monitoring is now more prevalent across

sectors. The EBA publicly consulted on Guidelines on the use of remote customer onboarding solutions[34] in 2021 and issued them in 2022.

76. The COVID-19 pandemic has created financial difficulties for businesses that might persist after the end of the pandemic. Risks linked to such businesses being taken over or given financial support by money launderers remain, especially in cash generating businesses. Several CAs underlined the consequences of economic turmoil contributing to ML/TF risks through the concealment or change of beneficial owner of illegally obtained assets.

77. As was the case in the 2021 Opinion, some CAs considered that the pandemic had a negative impact on the firms' AML/CFT compliance. They considered that, as a result of the reduction in revenues experienced during the pandemic, there was a risk that firms were forced to cut costs, reducing their staffing levels, including those responsible for AML/CFT compliance. At the same time, CAs' responses to questions relating to AML/CFT breaches identified in the different sectors in 2020 and 2021 did not suggest that this risk had crystallised.

78. The EBA, in its 2021 Opinion, found that the COVID-19 pandemic had led to a drop in CAs' supervisory activity, and an associated drop in levels of enforcement. Findings from the EBA's implementation reviews and AML/CFT databases, including EuReCA, suggest that supervisory activity is reverting to pre-pandemic levels, albeit with a greater prevalence of off-site reviews. According to most CAs, some adjustments made to accommodate pandemic restrictions on movement remain in place and have diversified the supervisory toolkit, including the use of virtual AML/CFT systems walk-throughs and the use of secure channels to sample test customer files.

3.2.8 Awareness of de-risking has increased but challenges remain

79. In 2022, the EBA published an Opinion on de-risking[35], in which it encourages competent authorities to engage more actively with institutions that de-risk and with users of financial services that are particularly affected by de-risking to raise awareness of the rights and responsibilities of both institutions and their customers. This recommendation has led increased awareness of de-risking, with several CAs carrying out an assessment of de-risking in their respective jurisdictions subsequently.

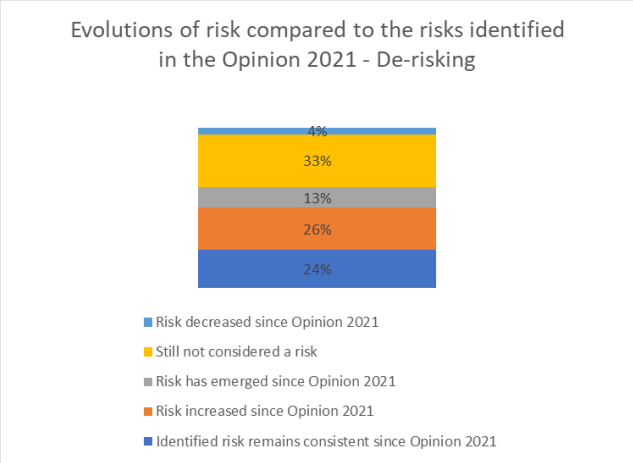
80. According to CAs, the categories of customers being de-risked have not changed significantly since the 2021 Opinion was published. However following Russia's invasion of Ukraine in 2022, the scale of de-risking of certain customer categories increased. This was the case in particular for refugees from Ukraine and individuals with links to Russia and Belarus, and some

34 Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849 - EBA/GL/2022/15

35 Opinion of the European Banking Authority on de-risking - EBA/OP/2022/01

commercial banks providing payments to Russia. The EBA took steps throughout 2022 to mitigate that risk[36] (see more in Box 1 of Section 3.1.3).

Figure 11: Evolution of risks in relation to de-risking



Box 8. EBA Guidelines to tackle unwarranted de-risking

In March 2023, the EBA issued two new Guidelines addressed to credit and financial institutions.

The first guideline amends the EBA ML/TF risk factors Guidelines[37] and outlines the steps that financial institutions should take to get a good understanding of how an individual NPO is set up and operates, as well as the factors they should consider when assessing the ML/TF risks associated with a business relationship with customers that are NPOs. These Guidelines aim at supporting the financial sector in its understanding of the specificities of prospective or existing customers who are NPOs.

The second guideline[38] clarifies the interaction between the access to financial services and institutions' AML/CFT obligations, including in situations where customers have legitimate reasons for failing to satisfy CDD requirements.

36 EBA statement on financial inclusion in the context of the invasion of Ukraine

37 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

38 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

Risks arising from legislative divergence and divergent supervisory practices

81. In its 2021 Opinion, the EBA highlighted concerns about the impact of divergent national legal frameworks and divergent supervisory practices on the EU's AML/CFT defences.

82. Supervisory convergence and cooperation have now increased following the implementation by CAs of the EBA's guidelines and recommendations, including those issued to CAs bilaterally in the context of the EBA's implementation reviews, but weaknesses remain.

3.2.9 AML/CFT supervisory coverage may not be adequate in all sectors

83. The 2021 Opinion pointed to risks arising from gaps in the AML/CFT supervisory framework that could have significant implications for the robustness of the EU's AML/CFT framework and for the integrity and stability of the financial markets. Furthermore, findings from the EBA's implementation reviews[39], the analysis of EuReCA submissions, AML/CFT colleges monitoring and the EBA's risk assessment of payment institutions and responses from CAs to the EBA's questionnaire (see more in Section 4 on ML/TF risks specific to each sector) suggest that challenges relating to the consistent application of a risk-based approach across the EU and the question of the adequacy of some CAs' approaches to AML/CFT supervision remain. In particular:

- CAs continued to experience challenges in operationalising the risk-based approach to AML/CFT supervision and make it effective. Most CAs had an incomplete understanding of the ML/TF risks in their banking sector and, despite the extensive resources devoted to the entity-level risk assessment, some competent authorities had not understood the purpose of the sectoral or entity-level risk assessment and did not use these assessments to update their supervisory approach.

- Other challenges to the effectiveness of the risk-based approach to AML/CFT supervision of banks include, translating ML/TF risk assessments into a comprehensive and risk-based supervisory strategy, finding the right balance between on-site and off-site supervisory tools, putting in place a sufficiently comprehensive supervisory manual and using a strategic approach for communicating with the sector.

- The number of specialist AML/CFT staff employed by CAs still varies significantly across the EU. While differences are expected and in line with the risk-based approach, the level of resources and AML/CFT supervision is not commensurate with the level of ML/TF risk and the size of the sector in all Member States. Differences in the frequency and intensity of supervisory engagements with firms in different sectors can be linked to differing risk levels in these sectors, but in some cases are due to resource constraints at the level of CAs.

39 EBA Report on CAs' approaches to supervision of banks with respect to the AML/CFT (round 3 – 2022) - EBA/REP/2022/08

84. In several sectors, a significant proportion of CAs indicated that they had not performed an assessment of the quality of the controls put in place by firms in these sectors, thus raising questions on the basis of which CAs assessed the residual risk profile of these sectors. As already pointed out in the 2021 Opinion, there is a risk that, in the absence of risk assessments, sufficiently intrusive inspections and the adequate, risk-based supervisory coverage of the whole sector, CAs may fail to identify, and act upon, ML/TF risks to which their sector is exposed.

3.2.10 Differences in CAs' approaches to assessing ML/TF risk associated with qualifying holdings create vulnerabilities

85. Findings from the EBA implementation reviews, the EBA peer review on the assessment of the acquisition of qualifying holdings[40], and from the EBA's report on the so-called Luanda Leaks[41] (see also Box 3 in Section 3.1.5) suggest that CAs' approaches to assessing ML/TF risk are not sufficiently robust in several Member States. This is in spite of the inclusion, in the 2016 Joint ESAs Guidelines on the prudential assessment of the acquisition of qualifying holdings[42], of a specific assessment criterion relating to ML/TF risks.

86. The consequence of such uneven national practices is that ML/TF risks may not be identified during the assessment process. They create a risk, which has crystallised in some cases, that criminals and their associates may own or control financial institutions.

87. The EBA intends to help CAs cooperate with each other for the assessment of notification of increase/decrease of acquisition of qualifying holdings taking place in a cross-border context, as per the future CRD6 and PSD3.

3.2.11 Cooperation has improved but more needs to be done

88. ML/TF risk cannot be tackled in isolation and AML/CFT and prudential supervisors both have a role to play. The revised Supervisory Review and Evaluation Process (SREP) Guidelines[43] set out the steps that prudential supervisors should take to tackle ML/TF risk and complete relevant provisions in EBA instruments on internal controls, suitability, qualifying holdings and

40 EBA Report on the peer review of Joint ESAs Guidelines on the prudential assessment of the acquisition of qualifying holdings, JC/GL/2016/01 – EBA/REP/2021/24

41 Report on competent authorities' response to the 2020 Luanda Leaks - EBA/REP/2022/05

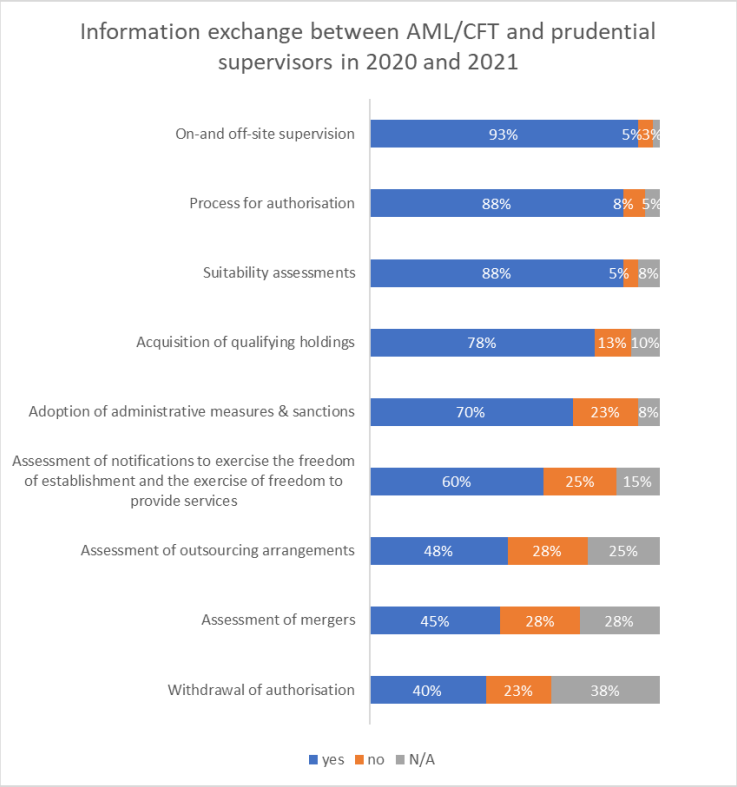
42 Joint ESAs Guidelines on the prudential assessment of the acquisition of qualifying holdings - JC/GL/2016/01

43 Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU - EBA/GL/2022/03

authorisation. Guidelines on the cooperation between AML/CFT and prudential supervisors and FIUs[44] were published in December 2021 (see more in box 10 of Section 3.3.3).

89. In its third Report on competent authorities' approaches to the AML/CFT supervision of banks[45], the EBA found that awareness of the synergies that exist between AML/CFT and prudential supervision had increased significantly since the first round of reviews. All AML/CFT and prudential authorities in this review round's sample had recently adopted measures to strengthen the information exchange between AML/CFT supervisors and prudential supervisors.

Figure 12: Information exchange between AML/CFT and prudential supervisors in 2020 and 2021



90. Cooperation between AML/CFT and prudential supervisors takes place at different stages of the supervisory cycle. Yet the degree of cooperation depends on the subject. 93% of AML/CFT supervisors that replied to the questionnaire suggested that they exchanged information with prudential supervisors for their off-site and on-site activities. However, only 60% of AML/CFT and prudential supervisors exchanged information during the assessment of notifications to exercise the freedom of establishment, and even though responses suggested that more than half of all supervisors exchanged information during core prudential processes such as assessments of applications for authorisation and qualifying holdings, EBA findings suggest

44 Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and FIUs - EBA/GL/2021/15

45 EBA Report on CAs' approaches to supervision of banks with respect to the AML/CFT (round 3 – 2022) - EBA/REP/2022/08

that input from AML/CFT supervisors was often not formalised, systematic or acted upon. This meant that ML/TF risks were not always identified or tackled.

Box 9. ESAs Report on the withdrawal of authorization for serious breaches of AML/CFT rules

In May 2022, the ESAs published a joint Report[46] on the withdrawal of licenses for serious breaches of the rules on AML/CFT.

The joint Report advocates for the introduction in all relevant EU sectoral laws of specific legal grounds to revoke licences for serious breaches of AML/CFT rules. The joint Report also calls for the inclusion of assessments by competent authorities of the adequacy of the arrangements and processes to ensure AML/CFT compliance as one condition for granting authorisation or registration. For this purpose, cooperation and information exchange between prudential supervisors and AML/CFT supervisors should be ensured.

91. Cooperation with other domestic authorities is also important but was not always adequate. This was in spite of most CAs having in place cooperation agreements. For example, only a small proportion of AML/CFT supervisors routinely obtained information to support their risk assessment from LEAs and tax authorities. This was in spite of the high prevalence of ML through tax crimes in many Member States.

92. Furthermore, emerging findings from the EBA's ongoing implementation reviews[47] suggest that with few exceptions, cooperation between CAs that are responsible for the AML/CFT supervision of the same institutions in the same Member State is largely ineffective. This appears to be the case in particular in Member States where one authority like the FIU, in its role as an AML/CFT supervisor, is supposed to assume a coordinating function, without adequate resources allocated to this task. In the absence of effective cooperation and coordination, AML/CFT supervision is disjointed with no clear strategy or priorities. Findings suggest that some institutions in these Member States are supervised by multiple authorities and exposed to divergent regulatory expectations, while others are not supervised at all.

Box 10. EBA Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and FIUs

In December 2021, the EBA published Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and FIUs[48] under Directive 2013/36/EU. Those Guidelines put in place the practical modalities of cooperation and information exchange between prudential supervisors, AML/CFT supervisors and FIUs, both at the level of Member States and across the EU's Single Market. In particular, the Guidelines facilitate and support cooperation and information

46 Joint ESAs Report on the withdrawal of authorisation for serious breaches of AML/CFT rules - ESAs 2022 23

47 EBA Report on CAs' approaches to supervision of banks with respect to the AML/CFT (round 3 – 2022) - EBA/REP/2022/08

48 Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and FIUs - EBA/GL/2021/15

exchange throughout the supervisory life cycle covering authorisations of new institutions, ongoing supervision including the risk assessment, and, where relevant, the imposition of supervisory measures and sanctions, including the withdrawal of the authorisation.

The establishment of AML/CFT Colleges since 2020 appears to have had a positive impact on the cooperation between AML/CFT supervisors, prudential supervisors and FIUs in different Member States. As of December 2022, 229 AML/CFT colleges in respect of different types of financial institutions were fully operating in the EU. Among these 229 colleges, 105 were established in 2022. Findings from the EBA's reviews show that competent authorities are increasingly making use of the information obtained via colleges when developing their AML/CFT supervisory plans and assessing ML/TF risk associated with the institution in their Member State.

Box 11. EBA Report on the functioning of AML/CFT Colleges in 2021

In September 2022, the EBA published its second report[49] on the functioning of AML/CFT colleges in 2021. The report highlights that competent authorities across the EU were committed to implementing the AML/CFT colleges' framework effectively. The EBA sets out its observations of good practices to help competent authorities enhance their future effectiveness. These include well-structured and organised college meetings by lead supervisors, pro-active participation and sharing of comprehensive information by some members and effective involvement of prudential supervisors in some colleges. As most colleges did not seem to have reached full maturity yet, the report identifies six actions that lead supervisors and permanent members of colleges should consider taking to enhance colleges' effectiveness, namely:

-finalising the structural elements of AML/CFT colleges, including the cooperation agreement and terms of participation of observers;
-enhancing discussions during the AML/CFT college meetings;
-fostering the ongoing information exchange within colleges;
-applying risk-based approach to college meetings;
-taking steps to identify areas for common approach or joint actions;
-enhancing supervisory convergence in AML/CFT colleges.

In Q3 2023, the EBA will publish its third report on the functioning of AML/CFT colleges in 2022. The EBA found that competent authorities have taken important steps to make AML/CFT colleges useful and effective. A structured approach to organising colleges meetings had contributed to the exchange of more substantive, actionable information than was the case previously, and prudential supervisors and FIUs actively participated in most AML/CFT colleges to which they had been invited. In several colleges, the quality of discussions was greatly enhanced, and the lead supervisor was leading these discussions much more effectively. A small number of colleges had taken coordinated actions to address areas of common concern with good outcomes.

49 EBA Report on the functioning of AML/CFT colleges in 2021 - EBA/REP/2022/18

3.2.12 Need for further convergence for the supervision of crowdfunding platforms under the AML/CFT framework

93. CFPs offer various types of fundraising models and include investment, lending, and donations. Not all models of CFPs carry the same ML/TF risks and not all are subject to AML/CFT requirements. To-date, 7 CAs are responsible for the AML/CFT supervision of 205 crowdfunding platforms that are obliged entities. 65% of those platforms are supervised by one CA. A further 70 crowdfunding platforms are registered in 4 Member States, but are not supervised for AML/CFT purposes.

94. CAs' assessment of the risk associated with CFPs has not changed significantly since the 2021 Opinion was published, though 13% of respondents suggested that this risk has emerged or increased. Examples provided by CAs included investment-based CFPs being vulnerable to risks arising from the collusion between the project owner and investor. In such situations, the investor may use illegally obtained funds to fund the investment project, for which the project owner has set an unrealistic funding target with no intentions to meet the target. When, as planned, the project fails to meet the target, clean funds are returned to the investor. They also included exposure to scam fundraising due to the ease with which it is possible to launch and market a crowdfunding project. CAs drew a correlation between fictitious investment projects and the lack of knowledge by crowdfunding service providers of the purposes of funding. Other examples provided by CAs included situations where individuals are asked to donate amounts for a seemingly lawful charitable project, such as humanitarian initiatives, which are thereafter used for terrorist financing purposes.

95. Moreover, CAs from Member States where CFPs are obliged entities and thus subject to AML/CFT supervision have raised concerns about the quality of CSP's AML/CFT policies and internal controls. They are particularly concerned about the effectiveness of CSPs' policies and procedures for the identification and verification of customers and beneficial owners. These risks can be increased due to the borderless nature of CFPs, which hinders the supervision by CAs of these CSPs and CFPs. In addition, CFPs' customers[50] or project owners[51] can be located anywhere in the world, including in high-risk jurisdictions.

96. CAs are also concerned about the systems and controls put in place by the CSPs to monitor and detect suspicious transactions. The main shortcomings relate to the lack of understanding by the CSPs of sources of funds used to fund projects and the purpose of the funding projects. In this regard, the use of less transparent means of payments, such as anonymous electronic money or virtual currencies, may increase the ML/TF risk. CAs also point out the lack of awareness of ML/TF risks by CSPs.

50 Any prospective or actual investor or project owner to whom a crowdfunding service provider provides, or intends to provide, crowdfunding services.

51 Any natural or legal person who seeks funding through a crowdfunding platform.

97. The new AML Package, once adopted, will expand the list of obliged entities to other sectors, including crowdfunding platforms that fall outside the scope of Regulation (EU) 2020/1503. Despite the fact that Regulation 2020/1503 already sets up some AML/CFT requirements in terms of due diligence, specifically of some crowdfunding service providers, that are complementary to the ones being set in the AML Regulation proposal, this may not be enough per se to effectively mitigate ML/TF risks. The ESAs, in their response to the European Commission's Call for advice on digital finance, called for a more robust approach to AML/CFT in this sector.

Box 12. Joint ESAs response to the European Commission's call for advice on digital finance

In February 2022, the three European Supervisory Authorities (EBA, EIOPA and ESMA) published a joint report[52] in response to the European Commission's February 2021 Call for Advice on Digital Finance.

Recommendation 6 highlights the need to support greater convergence in the identification and mitigation of ML/TF risks in a digital context. The ESAs recommend that the Commission assess as a priority whether to subject crowdfunding platforms licensed under Regulation 2020/1503 to EU AML/CFT legislation, in line with the EBA Report on the future AML/CFT framework in the EU. In addition, Guidelines on crowdfunding platforms (both outside and within the scope of Regulation (EU) 2020/1503) are required to clearly set out what adequate and coherent safeguards would look like, bearing in mind the nature of this activity. The ESAs recommend mandating AMLA to issue AML/CFT guidelines on crowdfunding. The existing EBA ML/TF Risk Factor Guidelines and the EBA Risk-based AML/CFT Supervision Guidelines already contain some sectoral guidelines for crowdfunding platforms and would, in the ESAs' view, be a useful basis in this regard.

Proposal: As set out in recommendation 6 of the Joint ESAs' response to the European Commission's call for advice on digital finance, the EBA advises the European Commission to assess whether to subject crowdfunding platforms licensed under Regulation 2020/1503 to EU AML/CFT legislation, in line with the requirement under Article 45(p) of Regulation 2020/1503.

3.2.13 Large cross-border cash transactions pose significant ML/TF risks

98. Several CAs identified cases of large cross-border cash transactions without apparent, legitimate economic purposes. Examples provided include large amounts of banknotes of non-euro currencies being exported to other Member States where they are then exchanged and transported back by courier to the initial Member State to large cash custodian banks.

99. Cross-border cash transactions can be legitimate, for example, because they are related to tourists exchanging cash on site during vacations, or because they are initiated by migrant

52 Joint ESA response to the EC's February 2021 call for advice on digital finance – ESA 2022 01

workers choosing to take their salary home in cash. They raise concern where their volume or amount is very high, and where explanations about the source of the funds are not plausible.

100. Investigations by law enforcement and tax authorities suggest that large amounts of cash transported to other countries are often the proceeds of crime. Eurojust[53] highlighted an organised crime group committing a complex tax-fraud scheme. The cash resulting from VAT and customs fraud offences committed in one Member State was collected and transported to another Member State, where the tax fraud was not a predicate offense nor was self-laundering a criminal offence. The transportation of cash also made it harder to prove that it was the result of a criminal activity.

101. The SOCTA Report from Europol[54] further indicate that large organised crime groups specialised in money laundering collect cash and transport it to credit institutions and other financial institutions at the layering stage of money laundering.

Proposal: The EBA advises CAs to take the steps necessary to understand their sector's risks in being used for cash-based money laundering.

3.2.14 Virtual IBANs can be abused for ML/TF purposes

102. Several CAs raised concerns about the use of virtual IBANs (vIBANs) for ML/TF purposes.

103. vIBANs can be used for different purposes, for example to counteract the effects of IBAN discrimination. They can also be used for reconciliation and record-keeping processes, for example in situations where big utilities companies manage a large number of customers and payments. However, because they are functionally identical to conventional IBANs and cannot be distinguished from them, they can make transaction monitoring and the detection of suspicious transactions difficult: transaction monitoring tools leverage on information incorporated in the IBAN, which in the case of vIBANs can be misleading. Europol identified several typologies of ML using vIBANs with a number of FIUs and LEAs.

104. CAs highlighted that there was a lack of legal certainty about AML/CFT supervision in situations where a financial institution set up a shell branch in a host Member State to issue local IBANs, but continues to collect funds directly through the parent financial institution on a free provision of services basis. This can raise questions about the applicable CDD and data-retention regime, the entity that is required to apply it, and the competent authority that is required to supervise it.

105. The EBA considers that the rules for creating and distributing virtual IBANs should be clarified to ensure that ML/TF risks that are specific to vIBANs are effectively managed.

53 Eurojust, Report on money laundering

54 Europol, Serious and Organised Crime Threat Assessment (SOCTA)

106. The EBA intends to further assess the risks associated with the misuse of virtual IBANS.

Proposal: If necessary, after the EBA's assessment of risks associated with the misuse of virtual IBANs, the EBA advises the European Commission and EU co-legislators to clarify supervisory expectations and competencies.

3.2.15 Future challenges with Instant payments for implementation of AML and restrictive measures

107. Instant payments (IPs) are electronic retail payments that are processed in real time, 24 hours a day, 365 days a year, where the funds are made available within 10 seconds for use by the recipient.

108. A common scheme (Single Euro Payments Area (SEPA) Instant Credit Transfer (SCT Inst)) and infrastructure (TARGET Instant Payment Settlement (TIPS)) for instant payments in euro exists since 2017. IPs are only offered by two thirds of EU PSPs and constitute about 11% of all Euro credit transfers in the EU[55].

109. On 26 October 2022 the Commission published a proposal[56] for a Regulation amending Regulations (EU) no 260/2012 (SEPA Regulation) and (EU) 2021/1230 (Cross-border Payments Regulation or CBPR2) as regards instant credit transfer in euro. PSPs offering a credit transfer service in euros will be required to offer IPs in euros. Payment institutions and e-money institutions that are not currently covered by the Settlement Finality Directive do not fall under this requirement but can offer IPs to their customers on a voluntary basis.

110. From the perspective of implementation of targeted financial sanctions, the proposal suggests screening all customers, immediately after entry into force of new or amended designations and at least once a day (Article 5d), rather than screening transactions (including the payee). This means that 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, like sectoral restrictive measures.

111. The proposal does not affect PSPs' obligations derived from the EU AML/CFT legislation. However, there might be situations where the ML/TF risk associated with a business relationship or transaction is increased, and where real-time transaction monitoring is the only effective AML/CFT control. IPs should be implemented on the basis of an assessment of associated risks in relation to money laundering, its predicate offences or terrorism financing, and not be driven by purely economic considerations in relation to the provision of such services.

55 Impact assessment on the Commission proposal for a Regulation on instant credit transfers in euros

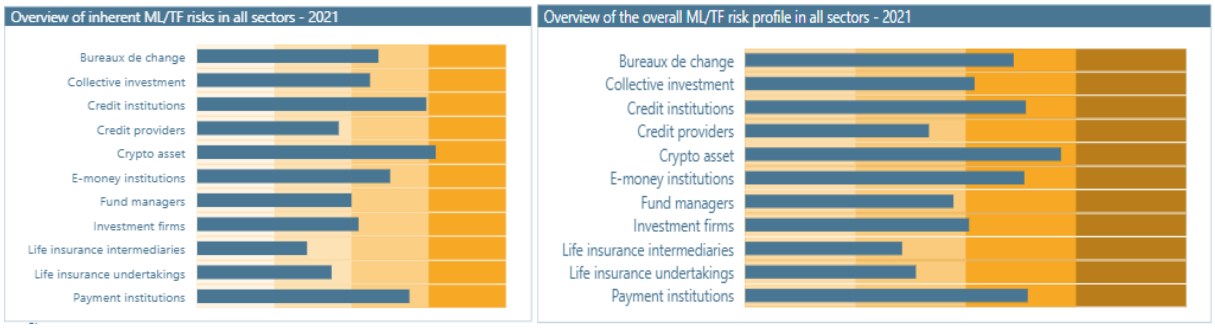
56 Proposal for a Regulation of the European Parliament and the Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro

<u>Proposal:</u> The EBA advises EU co-legislators to consider requiring payment service providers providing IPs to identify situations where IPs are not permissible on AML/CFT grounds and to refrain from providing IP services in those cases.

4. Money laundering and terrorist financing risks specific to each sector

112. The EBA assessed risks in each of the sectors under its AML/CFT remit. This section provides an overview of the main findings. Overall since the 2021 Opinion, the prevalence of inherent risks have not only increased across all sectors, but raise concerns of key AML/CFT controls that have not sufficiently improved in the same period. Assessment of risks has improved across sectors, and controls are increasingly put in place, even if CAs do not always assess their effectiveness positively. As emerging risks evolve quickly, more targeted supervision needs to be put in place.

Figure 13: Overview of inherent ML/TF risks and overall ML/TF risk profile in all sectors in 2021



4.1 Credit institutions

113. 33 CAs responsible for the AML/CFT supervision of 5 276 credit institutions (CI) responded to the EBA's questionnaire.

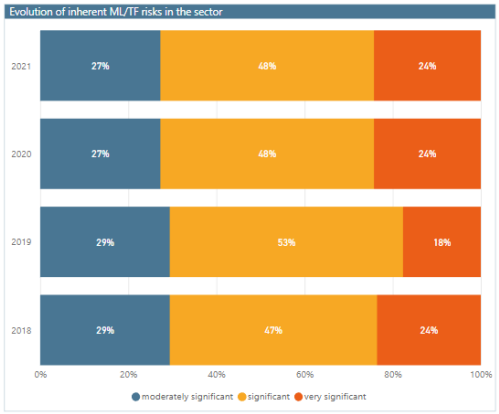
114. Overall, while CAs' assessment of both inherent and residual risks remained stable and suggests that the sector continues to present significant to very significant ML/TF risk, responses highlight ongoing concern about key AML/CFT systems and controls, which are often in place, but not always effective, for example the effectiveness of firms' transaction monitoring systems and the effectiveness of STR reporting. Management bodies also pay insufficient attention to compliance, hampering their operational functionality.

4.1.1 Inherent risks

115. More than 70% of CAs considered that the sector was exposed to a significant or very significant level of inherent ML/TF risk. This overall assessment has remained stable since 2019. Within the inherent risk category, responses suggest a reduction in inherent risks linked

to delivery channels and customers, and an increase in very significant inherent risk profiles linked to products and services.

Figure 14: Inherent ML/TF risks in the credit institutions sector

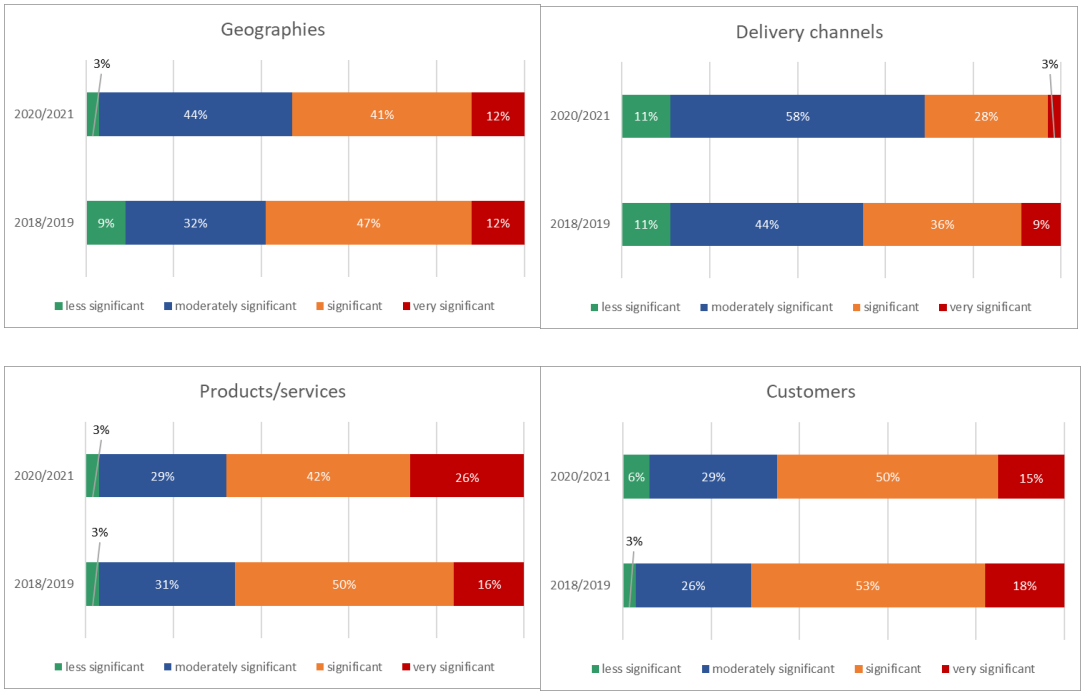


116. Levels and types of inherent risk differ among Member States due to contextual factors, such as the composition and size of the banking sector, the customer base and variations in the nature and prevalence of predicate offences such as corruption and tax crimes.

117. Notwithstanding these differences, all CAs that responded to the questionnaire pointed to risks related to products and services, and highlighted the ease with which money can be laundered through bank accounts. Examples provided included the abuse of bank accounts by money mules[57] in particular. ML risks linked to the use of cash remained a key concern in some Member States (see also Section 3.3.5 on large cross-border cash transactions), as does the perceived high, inherent ML risk associated with private banking and wealth management services especially for non-residents, correspondent banking and trade finance. A perceived ten-point increase in the level of very significant inherent risk in this category was linked to the growing provision of higher risk innovative financial products. CAs found that the digitalisation of business processes, the emergence of new business lines linked to FinTech and remote working had made credit institutions more vulnerable to cybercrime and computer fraud (see also Section 3.1.7 on ML of proceeds of cybercrime).

57 Europol, Money muling

Figure 15: Inherent ML/TF risk factors in the sector of credit institutions



118. More than half of all CAs that responded to the questionnaire consider that inherent geographic risk in the sector is significant or very significant. The nature of this risk varies in Member States, and ranges from risks linked to the operation of global banks with significant cross-border business to sectors with predominantly local banks and an important proportion of non-resident customers from higher ML/TF risk jurisdictions.

119. At the same time, some CAs' work to reduce the number of non-resident customers by requiring banks to reform their business models has contributed to an overall reduction in the perceived inherent risk associated with credit institutions' customers.

4.1.2 Quality of controls and overall risk profile

120. More than half of all CAs considered that the residual risk associated with the sector was significant or very significant. They found that the policies and procedures put in place by credit institutions were often adequate, but they were not always implemented or effectively applied. Customer risk assessments, transaction monitoring and STR reporting were particularly weak, with approximately one third of CAs assessing these controls as 'poor' overall. This mirrors early findings from the EBA's AML/CFT database, EuReCA, where 'material weaknesses' in individual credit institutions' CDD, transaction monitoring and approaches to suspicious transaction reporting represent nearly two third of all reports to-date.

121. Several CAs suggested that the adequacy institutions' AML/CFT governance had improved. Three quarters of all CAs suggested that this was now effective. Nevertheless, the outcome of the 2022 SREP cycle[58] highlights ongoing weaknesses regarding significant institutions' governance arrangements, which can have an impact on the effectiveness of an institution's AML/CFT systems and controls. Specifically, the ECB was concerned about the effectiveness of management bodies in their oversight role, as manifested by the absence of a strong challenging culture. Management bodies also pay insufficient attention to compliance, hampering their operational functionality.

Figure 16: Competent authorities' assessment of the quality of the controls in place in the sector of credit institutions

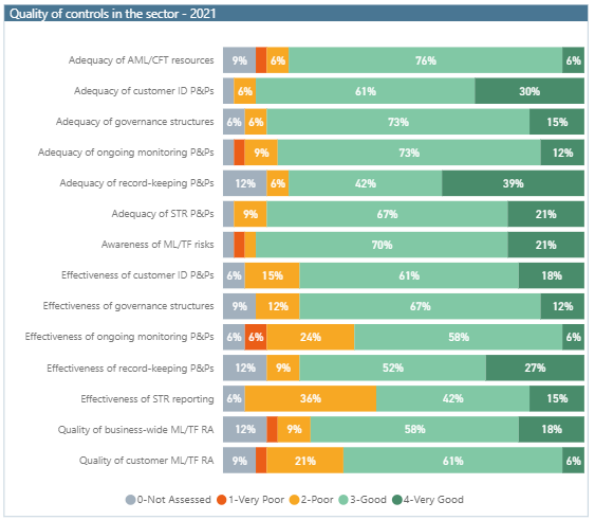
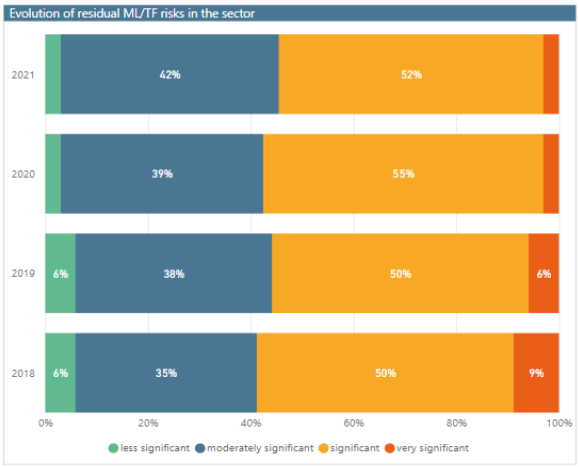


Figure 17: Evolution of residual risks in the credit institutions sector since 2018



4.1.3 Supervisory activities and breaches identified

122. CIs receive more supervisory attention than any other sector. This is in line with the size and complexity of the sector, the level of inherent ML/TF risk to which it is exposed and its role as entry point to other financial services. It is also reflected in the number of adverse findings reported to EUReCA.

58 Aggregated results of SREP 2022

Figure 18: Off-site and on-site inspections in the sector of credit institutions

123. The number and type of inspections is not always in line with the risk-based approach as CAs' responses suggest a focus on onsite inspections in credit institutions with a moderately significant or less significant risk profile, which is significant even when accounting for the greater number of institutions in these categories compared to the number of institutions in the higher risk categories. There was nevertheless a slight upward trend in the number of on-site inspections and off-site reviews of firms with a very significant risk profile between 2020 and 2021, although this trend is likely to also reflect the end of restrictions on movement imposed during the global pandemic.

124. In the EBA's second report[59] on CAs' approaches to the AML/CFT supervision of banks, the review team noted that most competent authorities were carrying out a small number of full scope on-site inspections each year and relied on off-site supervision for most other banks. With a few exceptions, the off-site supervisory measures CAs in the sample took were not intrusive and largely limited to a high-level review of banks' responses to CA's annual AML/CFT questionnaire. Monitoring of key indicators, such as banks' annual AML/CFT returns, is important, but is not a substitute for intrusive on-site or off-site AML/CFT supervision.

Box 13. EBA reports on competent authorities' approaches to the AML/CFT supervision of banks (round 2 2020/2021 and round 3 2022)

Over the course of 2020 and 2021, review teams assessed seven competent authorities from seven EU/EEA Member States and made recommendations tailored to each competent authority to support their AML/CFT work.

59 EBA report on competent authorities' approaches to the AML/CFT supervision of banks (round 2 2020/2021) - EBA/REP/2022/08

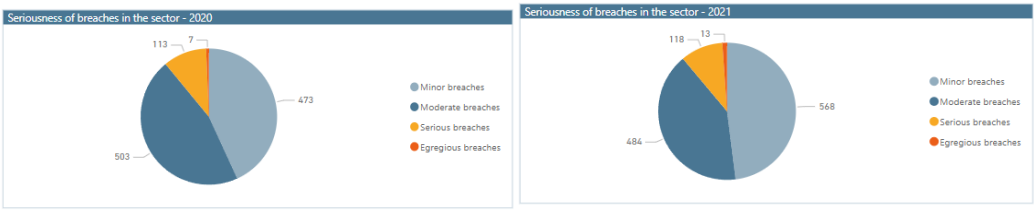
Among the common challenges that supervisors face, the EBA highlights difficulties in (i) identifying ML/TF risks in the banking sector and in individual banks; (ii) translating ML/TF risk assessments into risk-based supervisory strategies; (iii) using available resources effectively, including by ensuring sufficiently intrusive on-site and off-site supervision; and (iv) taking proportionate and sufficiently dissuasive enforcement measures to correct AML/CFT compliance weaknesses. The EBA also found that cooperation with FIUs was not always systematic and often ineffective. These challenges have hampered the implementation of an effective risk-based approach to AML/CFT supervision.

In 2022, review teams assessed[60] twelve competent authorities from nine EU/EEA Member States that are responsible for the AML/CFT supervision of banks. All competent authorities in this round had undertaken work to implement a risk-based approach to AML/CFT but significant differences existed in the way they identified and addressed ML/TF risks in banks. While some competent authorities had redefined their approach to AML/CFT supervision following high-profile ML/TF cases involving banks in their jurisdiction and were now largely effective, most competent authorities had not taken advantage of such opportunities or drawn on the lessons learnt by others, and therefore continued to face the same challenges as competent authorities that were part of the first two rounds of implementation reviews.

125. Most breaches found in the sector were rated as moderate or minor by CAs. They related to the effectiveness of transaction monitoring systems and the subsequent filing of STRs, the effective management of ML/TF risks including CDD, and internal controls including inadequate AML/CFT resources.

126. The total number of breaches decreased by 28% in 2020, due to a reduction in supervisory activities, including on-site inspections, during the COVID-19 pandemic. Data from EuReCA confirms that most deficiencies are detected during on-site inspections.

Figure 19: Seriousness of breaches identified in the credit institutions sector



4.1.4 Emerging risks

127. As was the case in the 2021 Opinion, a third of CAs identified the growing use of RegTech as an emerging risk. They were concerned that the move to remote onboarding during the pandemic without adequate safeguards had led to poor quality CDD.

128. Also a third of CAs referred to changes in banks' business models, which exposed these banks to ML/TF risk. This included a trend for mergers and acquisitions of smaller Fintech

60 EBA Report on CAs' approaches to supervision of banks with respect to the AML/CFT (round 3 – 2022) - EBA/REP/2022/08

companies by credit institutions, and the provision of 'Banking as a service' (BaaS), whereby credit institutions offer BaaS to multiple types of third parties ('white labelling'). CAs observed that it was challenging for credit institutions to integrate these new products and services in their AML/CFT framework and to adequately monitor and control the risks arising from such activities. It also included the growing embrace of crypto-assets as products or CASPs as customers. Section 3.2.2 has more details on this point.

129. Several CAs referred to ML/TF risks associated with vIBANs (see Section 3.3.6), cybercrime (see Section 3.1.7) and new types of laundromats using products such as digital payment services, e-money and digital banking.

130. Eight CAs confirmed findings in the EBA's 2022 Risk Assessment of the European Banking System that the increased focus on the implementation of targeted financial sanctions and restrictive measures means that institutions have shifted staff away from ML/CFT compliance to focus on restrictive measures instead[61].

Proposal: The EBA advises CAs to test the effectiveness of key AML/CFT controls in banks, including transaction monitoring systems and credit institutions' approaches to identifying and reporting suspicious transactions during inspections and if appropriate, as part of a thematic review. CAs should choose meaningful samples and use these to test system performance.

4.2 Payment institutions

131. In total, 32 CAs, which are responsible for the AML/CFT supervision of 3 140 obliged entities[62] in the sector of payment institutions (PIs), responded to the EBA's questionnaire.

132. CAs noted that AML/CFT internal controls of PIs have been improving but more progress is needed as those controls do not seem robust enough to mitigate the significant to very significant ML/TF risks. Supervisory practices at authorisation vary significantly and AML/CFT components are not consistently assessed. The use of agents by payment institutions carries a significant inherent ML/TF risk, especially in a cross-border context, yet there is no common approach to the AML/CFT supervision of agent networks.

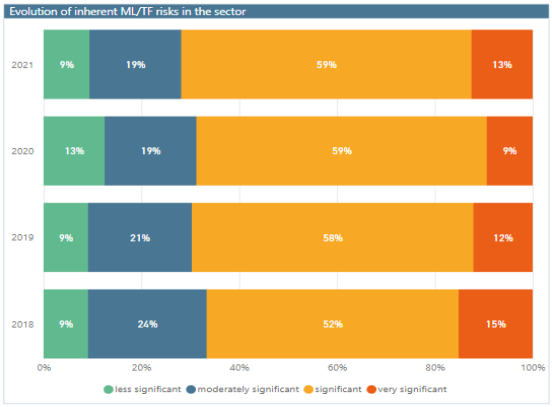
4.2.1 Inherent risks

133. Nearly three quarters of CAs that responded to the questionnaire consider that the inherent risk associated with the PI sector is significant or very significant. This constitutes a slight increase since 2018.

61 Risk Assessment of the European Banking System December 2022

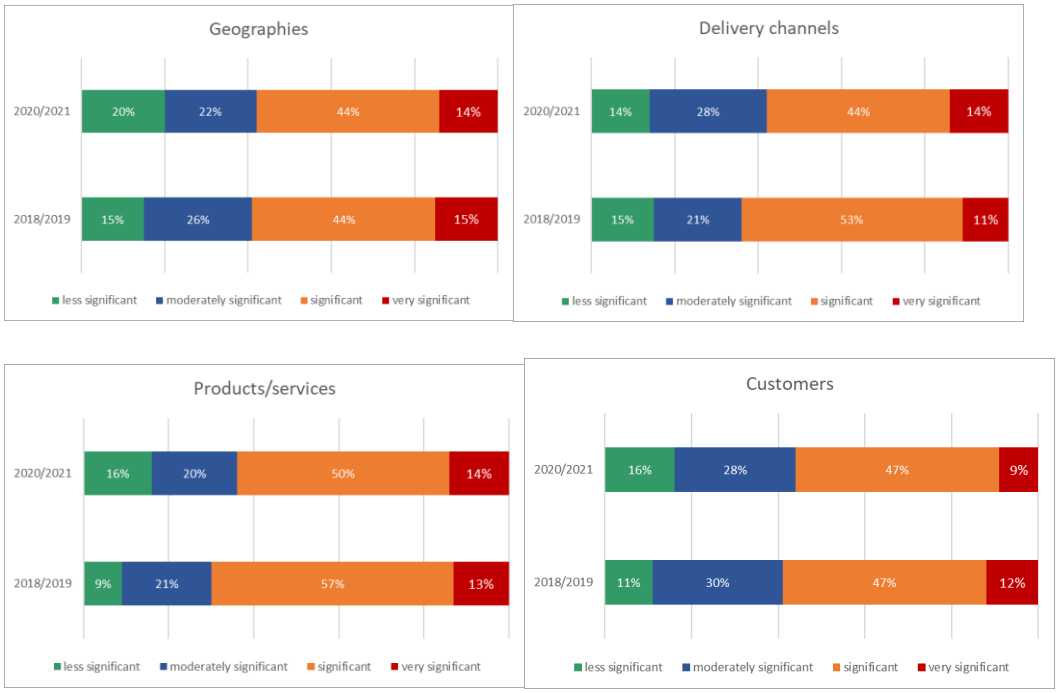
62 only the number of agents of payment institutions where they are obliged entities in their own right

Figure 20: Inherent ML/TF risks in the sector of payment institutions



134. On the contrary, according to CAs, the inherent risk associated with individual risk factors has since decreased.

Figure 21: Inherent ML/TF risk factors in the sector of payment institutions



135. The PI sector encompasses a large variety of institutions that carry different levels of inherent ML/TF risk. Money remitters remain associated with very significant ML/TF risk on account of their cross-border activity, whereas PISPs and AISPs, due to the nature of services they provide, are not exposed to significant ML/TF risks. Furthermore, contextual factors such as the proportion of immigrant populations from higher ML/TF risk jurisdictions that are likely to use payment services can affect the level of inherent risk in each Member State.

136. Similar to the 2021 Opinion, the most common factors that CAs identified as contributing to the high overall inherent risk rating of this sector include the cash-intensive nature of the services offered, the prevalence of occasional transactions rather than established business relationships, the high-risk jurisdictions in which or with which PIs operate, the large volume and high speed of transactions, the use of new technologies to facilitate the onboarding of customers remotely and the distribution channel used. Regarding the latter, CAs assessed the use of networks of agents in the sector as presenting particular risks.

Box 14. EBA's risk assessment on ML/TF risk associated with payment institutions

In 2023, the EBA published a risk assessment on ML/TF associated with the specific sector of payment institutions[63]. The purpose of this project was to assess 1. the scale and nature of the ML/TF risk associated with the sector; 2. the extent to which payment institutions' AML/CFT systems and controls are adequate and effective in tackling those risks; and 3. the extent to which current supervisory approaches are effective.

To complete this work, the 9a methodology requires the EBA to draw on information available to it. The risk assessment is desk-based, with information gathered from national competent authorities in the form of a questionnaire. It also included bilateral interviews with selected NCAs responsible for the supervision of the payments institution sector. In addition, information collected from NCAs in the context of the EBA's PSD2 peer review exercise (please refer to Box 15) on authorisation of payments institutions[64] also feeds in the 9a risk assessment.

The EBA's findings suggest that:

-ML/TF risk in the sector is not effectively managed.
-Not all AML/CFT supervisors base the frequency and intensity of on-site and off-site supervision on the ML/TF risk profile of individual payment institutions, and on the ML/TF risks in that sector.
-Supervisory practices at authorisation vary significantly and AML/CFT components are not consistently assessed. As a result, payment institutions with weak AML/CFT controls can operate in the EU and may establish themselves in Member States where the authorisation process is perceived as less stringent to passport their activities cross-border afterwards.
-There is no EU-level common approach to the AML/CFT supervision of agent networks, or the AML/CFT supervision of payment institutions with widespread agent networks. The use of agents by payment institutions carries a significant inherent ML/TF risk, especially in a cross-border context.

63 EBA Report on ML/TF risks associated with payment institutions - EBA/REP/2023/18
64 EBA Report on the Peer review on authorisation under PSD2 - EBA/REP/2023/01

4.2.2 Quality of controls and overall risk profile

137. CAs' assessment of the quality of the controls put in place by payment institutions suggests a small upward trend since the last Opinion was published in 2021. Nevertheless, two thirds of CAs view the residual ML/TF risk profile in the sector as significant or very significant overall. This is because according to CAs, controls in this sector are less effective than in any other financial services sector.

138. More than half of all CAs consider that ongoing monitoring and suspicious transaction reporting are not effective, and more than half of all CAs assess the quality of PIs' ML/TF risk assessments as poor overall, although some CAs suggested that, following increased supervisory engagement in their Member States, the quality of business-wide and individual ML/TF risk assessments had slightly improved. Serious concerns also exist in relation to PIs' governance structure, which more than 40% of CAs assess as inadequate and ineffective, and the sector's awareness of ML/TF risk, which nearly half of all CAs consider to be poor or very poor.

Figure 22: Competent authorities' assessment of the quality of controls in place in the sector of payment institutions

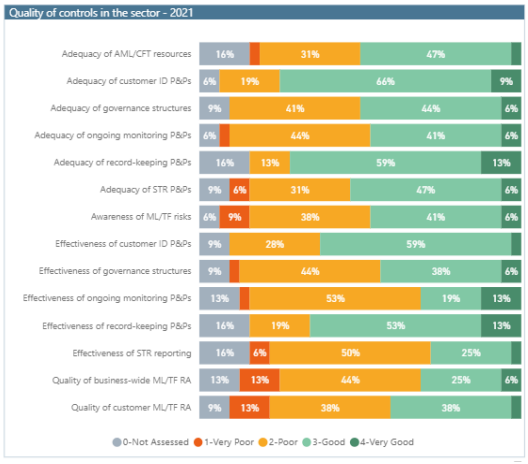
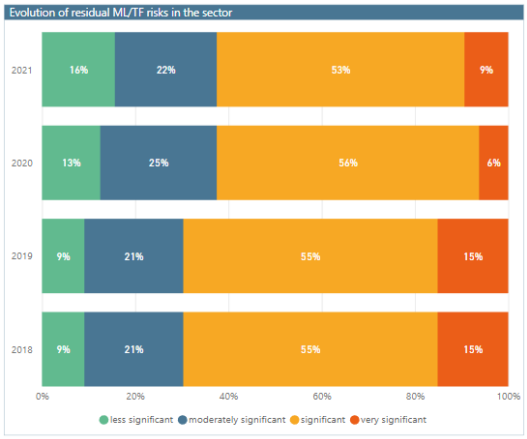


Figure 23: Evolution of residual ML/TF risks in the sector of payment institutions since 2018



Box 15: EBA peer review of authorisation of payment institutions and e-money institutions under the Payment Services Directive

In January 2022, the EBA published a peer review on authorisation of payment institutions and e-money institutions under the revised Payment Services Directive (PSD2)[65]. The review generally found increased transparency and consistency of the information required in the authorisation process. However, it also identified significant divergences in competent authorities' assessment and the degree of scrutiny of applications. The peer review included a specific chapter on the assessment of the applicants' internal AML/CFT control systems and measures and revealed divergences of supervisory practices across the EU Members on how the information collected in this context should

65 EBA Report on the Peer review on authorisation under PSD2 - EBA/REP/2023/01

be scrutinised and used. The review sets out a series of recommendations to address such divergences, in order to level out the supervisory playing field.

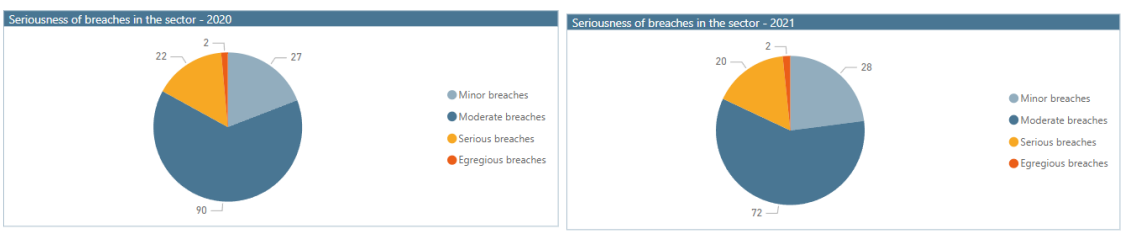
4.2.3 Supervisory activities and breaches identified

139. Almost all 32 CAs that responded to the questionnaire indicated they carried out some supervisory activity during 2020 and 2021. Most activities were carried out off-site, mainly through AML/CFT returns, data gathering surveys and scheduled reviews. On-site activities were mostly full-scope inspections, but the frequency, intensity and intrusiveness of supervisory engagement varied significantly between Member States and to a greater extent than could have been justified on a risk-based approach. For example, 1 CA accounts for two thirds of all full-scope inspections in 2020 and half of all full-scope inspections in 2021.

Figure 24: Off-site and on-site inspections in the sector of payment institutions

140. The low number of intrusive supervisory actions goes some way towards explaining the number of breaches identified. Nevertheless, according to EuReCA, payment institutions constitute the second most reported sector where 'material weaknesses' were identified, after credit institutions.

Figure 25: Seriousness of breaches identified in the sector of payment institutions



141. Most breaches in the sector related to ongoing monitoring, internal controls and overall AML/CFT policies and procedures, customer identification and verification and customer and business-wide risk assessment. This is broadly in line with the quality of controls that CAs were generally concerned about.

142. The most common supervisory measures used across CAs to mitigate weaknesses in firms' AML/CFT systems and controls included imposing a fine or administrative/pecuniary sanction, a warning, requiring the firm to put in place a remediation plan, or implement specific measures. However, where breaches were egregious, the CAs applied more robust measures, including the withdrawal of authorisation which took place two times in total between 2020 and 2021.

4.2.4 Emerging risks

143. The increasing use of new technologies, including AI, for the purpose of remote onboarding and digital identification is considered by most CAs as an emerging risk. Ongoing, serious systems and controls weaknesses in the sector suggest that payment institutions' ability to mitigate those risks effectively are limited.

144. Some CAs raised concerns about 'white labelling'. A growing number of payment institutions make their license available to independent agents who develop their own product under the license of the regulated financial institution. Ultimately, this can result in the provision of a broad range of financial products, which inspection findings suggest are not always monitored sufficiently.

145. Third party merchant acquiring has been identified as an emerging trend, and potentially a new ML/TF risk. In this setting, the merchant acquirer (which is the entity providing payments processing services to merchants including authorisation, clearing or settlement) outsources certain parts of the acquiring process to a TPA, which are oftentimes obliged entities themselves. TPAs then perform services for the merchant on the acquirer's behalf and are responsible for complying with the AML/CFT laws of the respective jurisdiction (within or outside the EU) when onboarding and monitoring the merchant. It puts the acquirer at risk of indirectly processing illicit funds through the TPA if the TPAs AML/CFT programme is vulnerable to ML/TF and/or sanctions violations. TPA transactions cause a segmentation of the acquiring business resulting in an increased ML/FT risk, including transaction-based laundering, or risk of other fraudulent activities.

146. Finally, as was the case for credit institutions, CAs highlighted the use of virtual IBANs (vIBANs) and the use of payment institutions to circumvent restrictive measures as both, current and emerging risks. Section 3.3.6 on vIBANs and Section 3.1.2 on restrictive measures have further details on these points.

<u>Proposals:</u> The EBA advises CAs to assess how to provide targeted guidance to the sector to ensure that supervisory expectations regarding adequate and effective AML/CFT systems and controls are well understood and applied. The EBA's Risk Factors Guidelines contain further details.

The EBA advises CAs to review their approach to the AML/CFT supervision of payment institutions to ensure that it is sufficiently risk-based and intrusive, in line with provisions in the Risk-based AML/CFT Supervision Guidelines. CAs should focus more on the supervision of agent networks and cooperate with their counterparts in case of cross-border agent networks.

4.3 E-money institutions

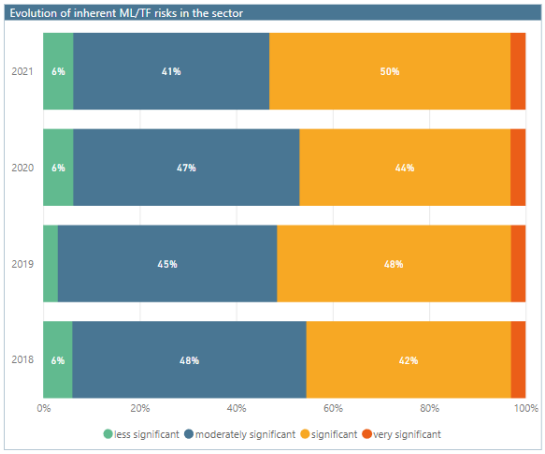
147. In total, 32 CAs responsible for the supervision of 428 EMIs responded to the EBAs' questionnaire. This sector is highly concentrated, with more than half of all EMIs based in 6 Member States.

148. Most CAs considered the sector to present significant or moderately significant inherent ML/TF risks. According to CAs, the main contributing factors are those associated with distribution channels and geographies, which both increased since the 2021 Opinion. CAs are also concerned about the sector's use of innovative technology with limited AML safeguards.

4.3.1 Inherent risks

149. More than half of all CAs assess the inherent risk associated with EMIs as significant or very significant.

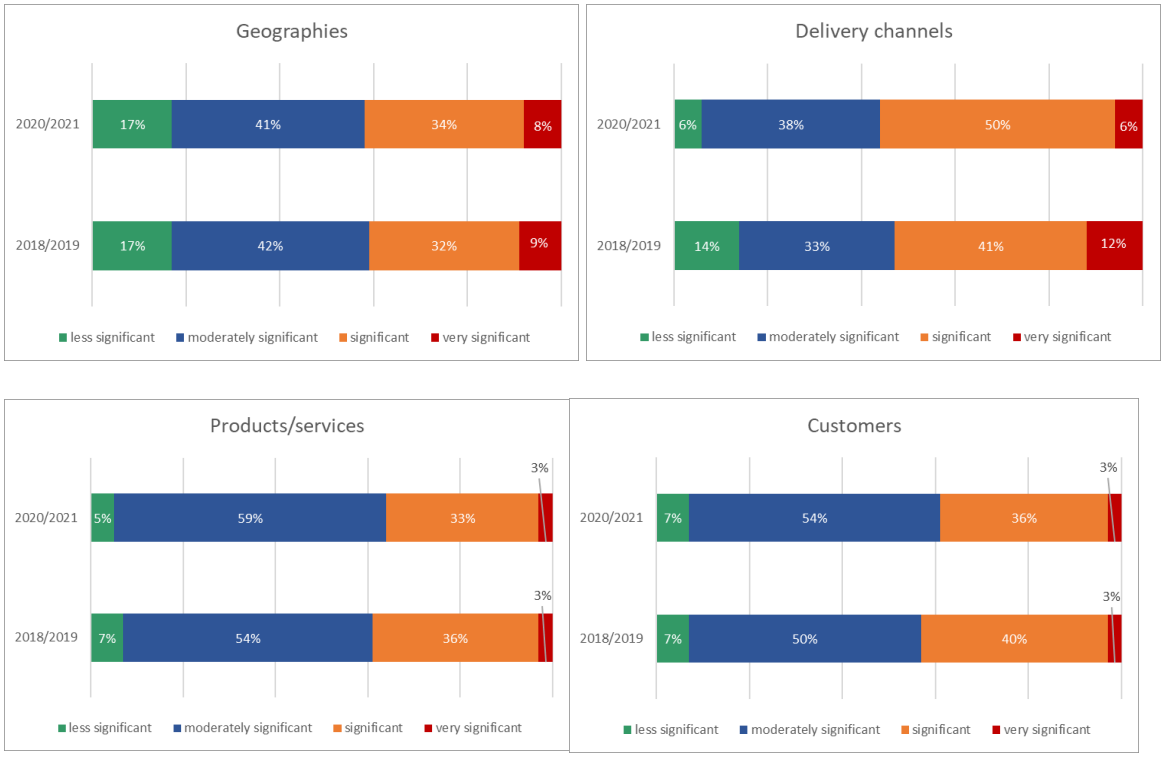
Figure 26: Inherent ML/TF risks in the sector of e-money institutions



150. CAs' responses to questions about individual inherent risk factors have remained broadly unchanged since the 2021 Opinion was published. Nevertheless, there has been a small upward trend in risks linked to delivery channels, which more CAs than before assess as significant. This is because of the emergence of new distribution channel risks, including the growth in white label products. Some CAs highlighted the non-uniform interpretation and application of the term distributor from Directive 2009/110/EC (2EMD), and ongoing concerns about inherent risks relating to the sector's extensive reliance on non-face-to-face identification processes, which was amplified after the COVID-19 outbreak. Upward trends have also been noted in the context of certain fraud typologies including fake shop fronts, and crypto investment fraud which are directly linked to e-payment accounts.

151. CAs raised particular concerns about prepaid cards in situations where there is no upward limit to the number of cards a customer can hold, or prepaid cards and other products offered by EMIs that allow high-value or unlimited value payments, loading or redemption, including cash withdrawal. Risks associated with anonymous e-money issued in third countries, which exceed national thresholds and for which lower identification standards are required, were also highlighted. A related risk is close links of some EMIs with specific higher-risk activities like online gambling companies, loan providers, crypto-asset service providers, among others.

Figure 27: Inherent ML/TF risk factors in the sector of e-money institutions



152. Almost half of all CAs assessed the sector's exposure to ML/TF risk associated with cross-border transactions as significant. Many CAs raised concern about risks related to servicing online customers from third countries, potentially leading to higher fraud risks. Several CAs indicated that EMIs were exploiting the passporting regime by establishing themselves in a Member State with less robust AML/CFT controls, or by failing to notify the presence of a physical network or to establish a central contact point where local law requires this.

4.3.2 Quality of controls and overall risk profile

153. Half of all competent authorities considered the residual risk in the sector as significant or very significant. This constitutes an increase in perceptions of residual risks since 2018. This increase is due in part of more competent authorities carrying out a formal risk assessment of the sector than was the case in the 2021 Opinion, but serious concerns about the adequacy and effectiveness of EMIs' AML/CFT systems and controls remain.

154. CAs are most concerned about the effectiveness of ongoing monitoring policies and procedures and the effectiveness of STR reporting. They also raised concerns about the quality of EMIs' business-wide and customer ML/TF risk assessment. A 2021 report by the Belgian FIU[66] suggests that the risk-based approach of PSPs is mainly oriented towards the absolute value of transactions, which makes it attractive to terrorist financing considering that the latter typically concerns lower amounts.

155. The use of intermediaries in the distribution chain is common in the sector, which can make adequate AML/CFT controls and oversight more difficult. Some CAs highlighted the non-uniform interpretation and application of the term distributor from Directive 2009/110/EC (2EMD).

Figure 28: Competent authorities' assessment of the quality of the controls in place in the sector of e-money institutions

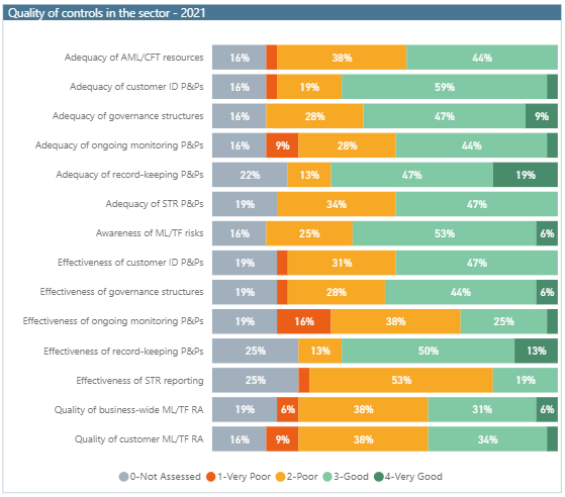
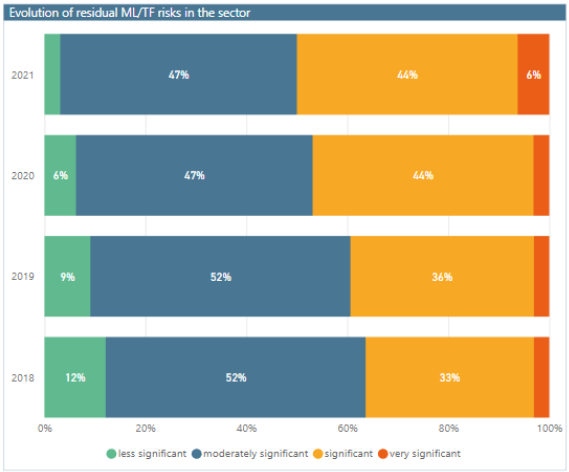


Figure 29: Evolution of residual ML/TF risks in the sector of e-money institutions since 2018



4.3.3 Supervisory activities and breaches identified

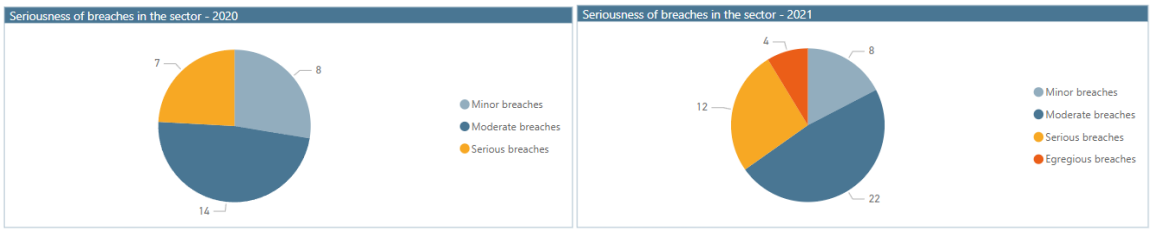
156. Most CAs relied on off-site supervisory activities, mainly AML/CFT returns, but some CAs also scheduled off-site reviews and thematic off-site reviews. They relied less on on-site supervision of the sector. Where these took place, they consisted mostly of on-site engagements, such as meetings with compliance officers, rather than intrusive inspections.

66 CTIF CFI Annual Report 2021

Figure 30: Off-site and on-site inspections in the sector of e-money institutions

157. As a result of their supervisory activities, CAs identified almost twice as many breaches in 2021 than in 2020. In 2020, where breaches were identified, these were mostly moderate. In 2021, breaches identified were mostly serious, with a few egregious breaches reported.

Figure 31: Seriousness of breaches identified in the sector of e-money institutions



158. The most common breaches in the sector related to the customer identification and verification, ongoing monitoring, internal controls and overall AML/CFT policies and procedures, including transaction monitoring, and customer risk assessments. This is in line with the controls about which CAs were generally concerned.

159. Feedback from CAs points to divergent approaches by CAs in cases of identified egregious breaches. Only 1 CA imposed a fine/administrative pecuniary sanction, while some CAs, for instance, indicated they had issued a warning, orders to comply, orders to put in place a remediation plan and/or orders to implement mitigating measures, while other CAs applied a restriction of business relationships with certain customers.

4.3.4 Emerging risks

160. The sector is characterised by the constant and rapid development of innovative products and services and the use of new technologies which might have less effective safeguards and be more prone to being exploited for ML/TF purposes. Moreover, the use of technology can pose challenges to the AML supervisors, who may lack the technical skills to

assess the adequacy of technological solutions for AML/CFT purposes. The growing adoption of blockchain and analogous technologies could further hamper the ability of CAs to have effective oversight due to the decentralisation of service providers.

161. CAs highlighted risks associated with the EMIs providing crypto-asset services with an insufficient knowledge of applicable regulation. Those services are often offered via a group structure arrangement on an outsourcing basis, with blurred lines on the separation of governance and operations.

162. CAs noted the rising trend of white labelling, with EMIs making their licence available to independent agents who develop their own product under the licence of the regulated financial institution. Ultimately, this results in a broad range of financial products. CAs suggested that it was challenging for e-money institutions to integrate these products and corresponding risks in their AML/CFT framework and to adequately monitor and control the risks arising from such activities.

163. The risk of non-implementation of targeted financial sanctions was raised as an emerging risk by most CAs.

Proposals: The EBA advises CAs to base the frequency and intensity of on-site and off-site supervision on the ML/TF risk profile of individual e-money institutions, and on the ML/TF risks in that sector.

The EBA advises CAs to assess how 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.

4.4 Bureaux de change

164. Twenty-three CAs that are responsible for the AML/CFT supervision of 6,619 firms providing currency exchange services (bureaux de change – BdC) responded to the EBA's questionnaire in respect of both 2020 and 2021. The BdC sector is concentrated in Member States outside of the Eurozone, with 65% of the BdC based there.

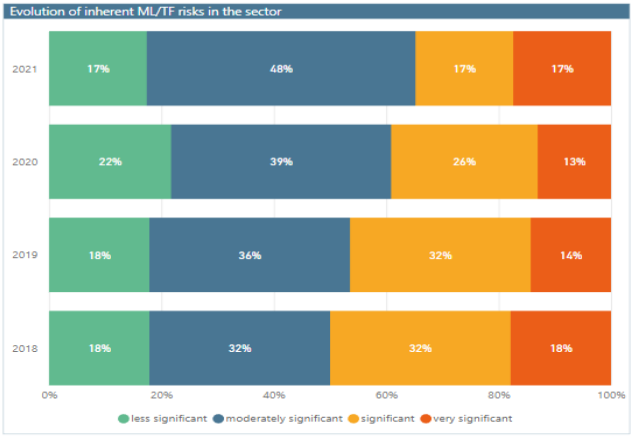
165. The majority of CAs considered the sector as presenting moderate risks from an inherent risk perspective. A large proportion of CAs indicated that they had not performed supervisory activities.

4.4.1 Inherent risks

166. The BdC Sector is considered as presenting moderately significant risks by around half of CAs from an inherent risk perspective. This represents a shift compared to the 2021 Opinion, when half of CAs considered the sector with a significant to very significant risk profile. At the

time, most CAs had not carried out a formal risk assessment of the sector, but this had now changed.

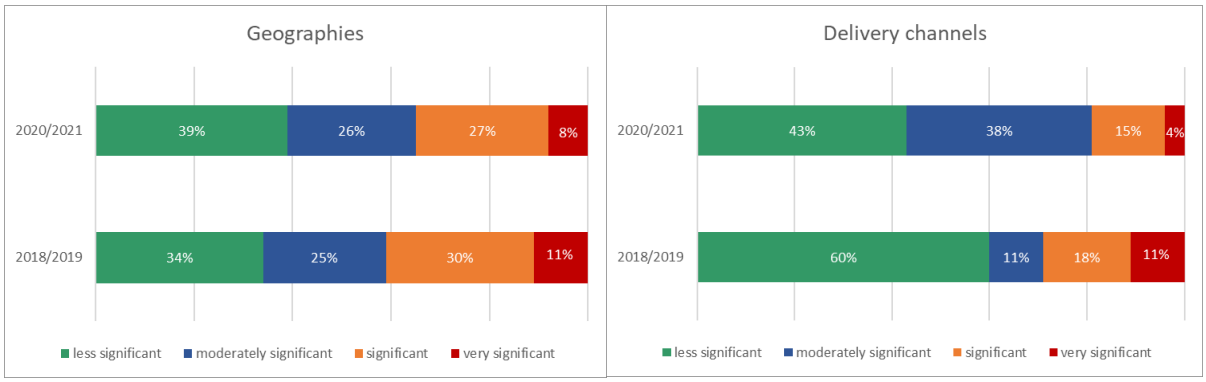
Figure 32: Inherent ML/TF risk profile in the sector of bureaux de change

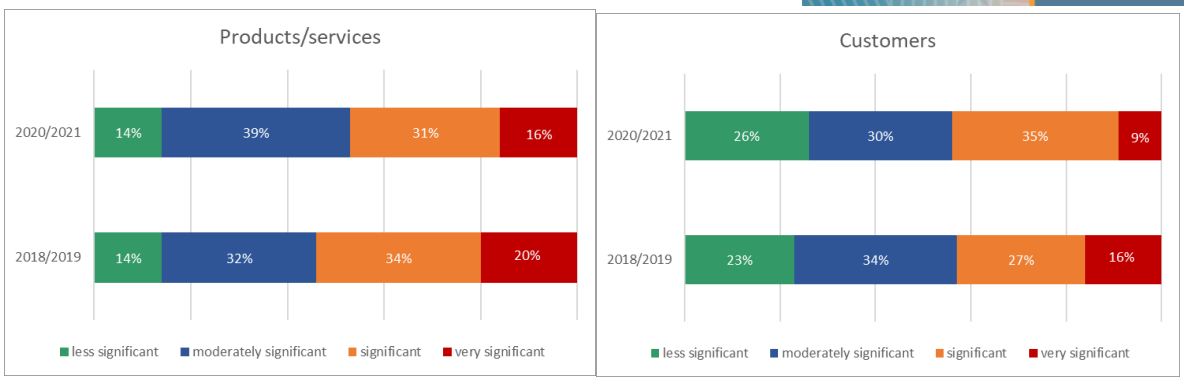


167. The key inherent risks in the sector relate to the cash-intensive nature of the business and the nature of its customers that often include itinerant and occasional customers, for example immigrants, asylum seekers, cross-border workers and tourists. Those ML/FT risks are increased with transactions conducted in bureaux de change used by a large number of random customers, like the ones located in commercial centres of big cities and tourist centres.

168. CAs indicated that a number of entities within the sector might be owned or controlled by criminals and used to launder large sums of cash. Other risks are related to additional services offered by BdCs like transfers of funds to third party foreign exchange accounts or foreign exchange associated with transfer of gold via mail or via any other intermediary offering parcel delivery services. Such activities generate a risk that the beneficial owner of the transaction is not identified.

Figure 33: Inherent ML/TF risk factors in the sector of bureaux de change





169. CAs also highlighted geographical risk associated with the levels of activities occurring near border regions, in particular near the Schengen zone borders and associated cash-intensive operations as a key risk-increasing factor for the sector. Some CAs identified specific risks related to predicate offences, such as migrant smuggling and terrorist financing, the influx of refugees from third countries, and the lack of information about the destination of funds exchanged.

4.4.2 Quality of controls and overall risk profile

170. Following the adoption of formal risk assessments, most CAs rated the controls put in place by firms in the sector as good overall, compared to poor in the previous Opinion on ML/TF risk. CAs considered that the adequacy and effectiveness of identification and verification policies and procedures had largely improved but rated the effectiveness of ongoing monitoring and suspicious transaction reporting as poor overall.

171. The evolution of residual risks has deteriorated in 2020 and 2021, with an increase of significant risks. It seems controls are in place but they do not effectively mitigate inherent risks.

Figure 34: Competent authorities' assessment of quality of controls in place in the sector of BdC

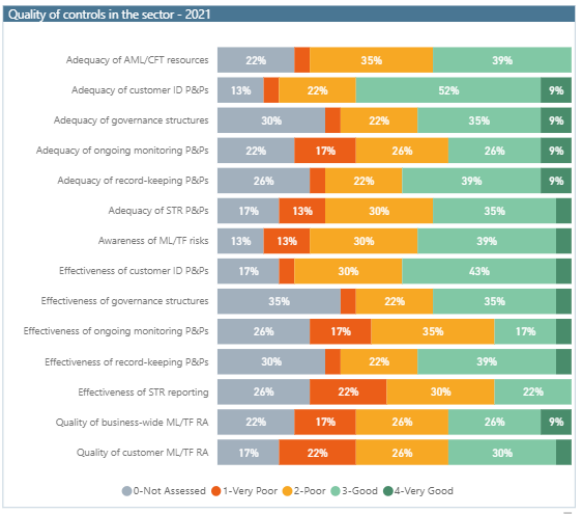
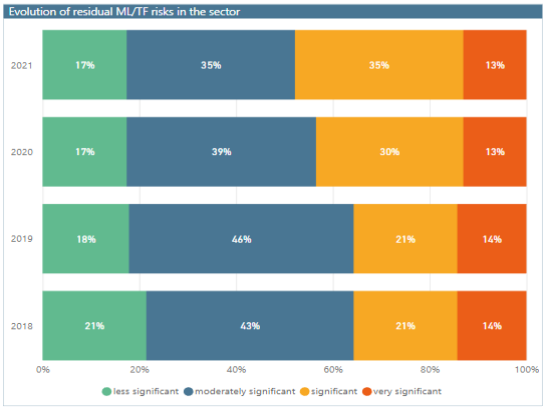


Figure 35: Evolution of residual ML/TF risks since 2018 in the sector of bureaux de change



4.4.3 Supervisory activities and breaches identified

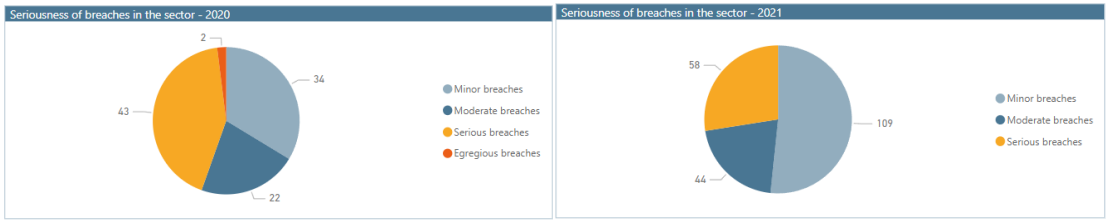
172. The sector is subject, across the EU, to very divergent supervisory approaches among CAs. It is noticeable for instance that a large proportion of CAs indicated they had not performed supervisory activities or had performed only a limited number.

173. When inspections are carried out, it seems that CAs mostly performed full-scope inspections. This high proportion is due to 1 CA with the largest sector which performed 83% of all on-site supervisory activities. Other CAs conducted targeted or thematic inspections, which could explain an apparent narrow focus of supervision: for example, more than one third of all supervisors had not assessed the adequacy and effectiveness of governance structures, whereas customer identification and verification policies and procedures featured in more than 80% of all inspections.

Figure 36: Off-site and on-site inspections carried out by competent authorities in the sector of bureaux de change

174. CAs identified a relatively small number of breaches in the sector in 2020 and 2021, which were either mainly rated as minor or serious. The number of breaches identified increased substantially in 2021, after a drop in the number of supervisory activities during the COVID-19 pandemic in 2020.

Figure 37: Seriousness of the breaches identified in the sector of bureaux de change



175. From the responses received, it appears that the main breaches in this sector correspond to the controls that CAs were generally concerned about, such as internal controls and overall AML/CFT policies and procedures, ongoing-monitoring and suspicious transaction reporting. Breaches in relation to customers' identification decreased between 2020 and 2021, which is in line with the assessment of controls.

176. Feedback from competent authorities suggests that minor breaches are usually followed by warnings or order to implement measures. On serious breaches, the approaches followed appear to be more diverse. In these cases, CAs mostly applied additional measures such as fines/administrative pecuniary sanctions, public statements, orders to comply and orders to implement measures.

4.4.4 Emerging risks

177. CAs did not identify specific emerging risks in this sector. The cash-based nature of the sector's business and the sector's limited understanding of their AML/CFT obligations were identified by CAs as an ongoing source of concern.

178. Some CAs raised the issue of ineffective screening procedures for restrictive measures, due to the poor IT infrastructure in some small BdCs.

Proposal: The EBA advises CAs to ensure a sufficiently broad view of AML/CFT systems and controls, especially where bureaux de change offer other financial services such as gold and precious stones trading.

4.5 Investment firms

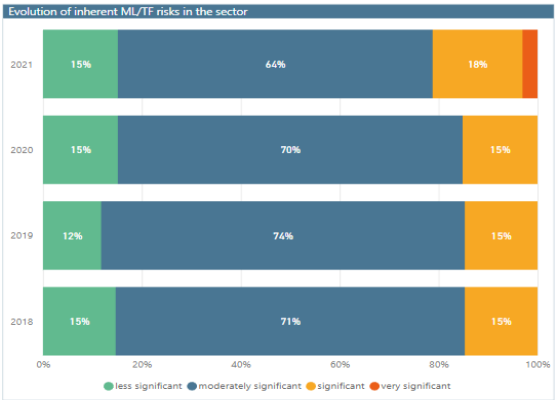
179. The EBA received responses from 32 CAs responsible for the AML/CFT supervision of investment firms for both years under review (2020 and 2021), covering a total of 3 283 investment firms.

180. CAs rated the overall inherent risk of the sector as moderately significant. A key inherent risk is the sector's significant exposure to tax-related crimes. CAs indicated that the quality of key controls for the sector, such as the quality of business-wide and individual risk assessments, remained good overall.

4.5.1 Inherent risks

181. The majority of CAs have rated the overall inherent risk profile of the investment firms' sector as moderately significant. The sector's exposure to ML/TF risk has remained substantially unchanged since the 2021 Opinion, although one CA assessed the sector as presenting very significant risks in 2021.

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



182. The analysis of the individual risk factors shows that all categories of risks have been rated by most CAs as posing a moderately significant risk. This is similar to the 2021 Opinion. However, some CAs rated customer, geographies and delivery channel risk as very significant

for the first time in 2021. CAs expressed concerns related to the customer risk exposure, which appears to be further increased in view of the exposure to high-net-worth individuals and the difficulties that firms may encounter in understanding the source of wealth and source of funds of customers, including non-resident customers.

183. Investments firms are often exposed to significant risks related to tax-related crime. This is especially the case when customers are repatriating funds from abroad (tax havens) and when investment firms do not have access to adequate know-how to identify and assess the source of wealth and funds and to make sure that related tax obligations have always been respected in the past, both regarding the wealth and the related income.

184. Among the products offered by the sector, there is a wide diversity of complex products, which can be used for illicit purposes. Risks specific to the sector include insider trading and market abuse risk, misuse of companies' assets with investments in companies based in countries at risk, investment in high-risk industrial sectors and mirror trading scams. Some CAs highlighted the misuse of money accounts tied with securities accounts, either to invest proceeds stemming from illegal activities, most of the time by strawmen and shell entities (e.g. registered in tax havens), or to transfer money from illegal activities among different accounts.

Figure 39: Inherent ML/TF risk factors in the sector of investment firms

185. The number of CAs assessing inherent geographical risk as significant has increased since the 2021 Opinion. This may be attributed to customer funds generated by activities in high-risk jurisdictions and/or funds transferred from financial institutions in high-risk jurisdictions.

186. However, most of the CAs assessed this sector as having moderately significant inherent exposure to ML/FT risks arising from cross-border activities. Compared to the 2021 Opinion, no CAs indicated a very significant risk associated with cross-border activities of the sector.

4.5.2 Quality of controls and overall risk profile

187. A large proportion of CAs had not carried out a formal risk assessment of the sector. Overall, they assessed the quality of controls within the investment firms' sector as good. This assessment is similar to the one of the 2021 Opinion.

188. CAs appeared to be satisfied in particular with the controls related to the adequacy and effectiveness of customer ID policies and procedures, which have improved since the 2021 Opinion. The effectiveness of STR reporting and ongoing monitoring also increased, though more than 40% of CAs considered this to be 'poor' or 'very poor'. The quality of business-wide and individual risk assessment remains a concern for approximately one third of all CAs.

189. In spite of this, nearly 80% of all CAs assessed the overall risk profile of the sector as moderately significant.

Figure 40: Competent authorities' assessment of the quality of controls in place in the sector of investment firms

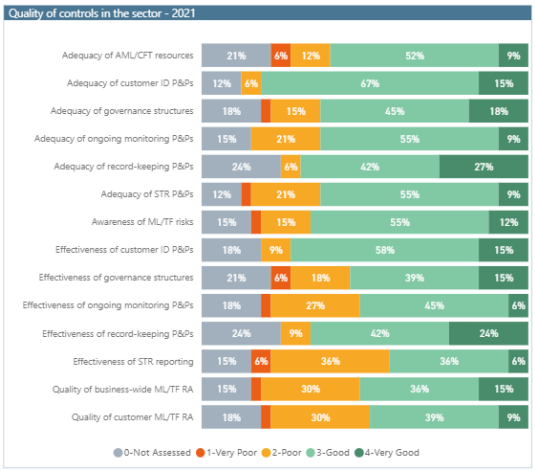
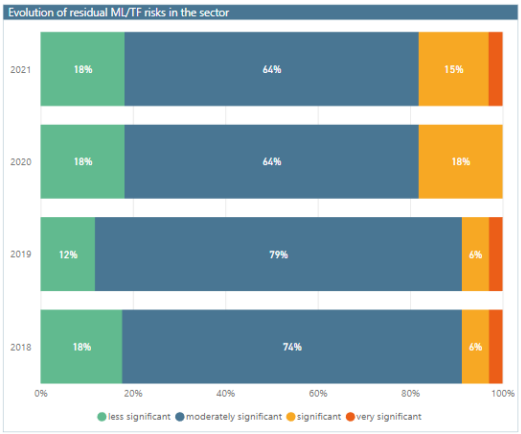


Figure 41: Evolution of residual risk profile in the sector of investment firms since 2018



4.5.3 Supervisory activities and breaches identified

190. Most CAs used AML/CFT returns and scheduled off-site reviews as their preferred off-site tool. CAs favoured scheduled full-scope inspections for their on-site reviews.

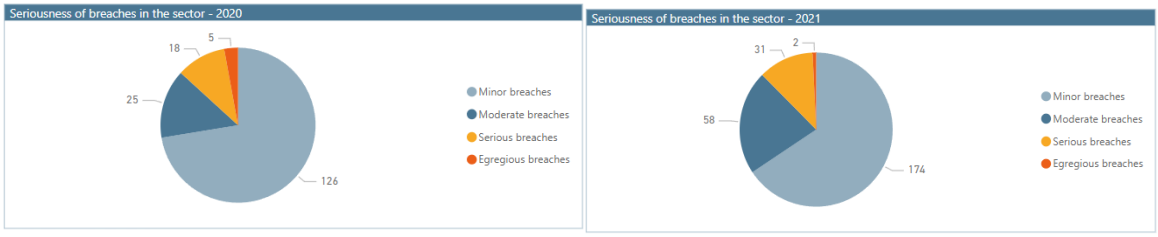
191. In 2020, due to the COVID-19 pandemic, half of the CAs indicated they temporarily changed the method of carrying out on-site inspections, using remote-tools like direct IT-access into institution´s core systems, data uploads into secure file-sharing platforms and interviews through video calls. One third of CAs decided to continue on-site inspections in a hybrid mode from 2021 on.

Figure 42: Off-site and on-site inspections in the sector of investment firms

192. CAs appeared to have concentrated their supervisory activities on firms rated to a less significant risk profile, in line with the number of firms rated by CAs in that risk category. Less focus, in both off-site and on-site inspections, was placed on firms presenting significant and very significant risks.

193. The breaches found by CAs in the sector were, in large part, minor breaches.

Figure 43: Seriousness of the breaches identified in the sector of investment firms



194. The most common types of breaches found in the sector identified by CAs in 2020 and 2021 related to the customer identification and verification, internal controls weaknesses (including overall AML/CFT policies and procedures), customer risk assessment and weaknesses in suspicious transaction reporting. This is similar to the findings of the 2021 Opinion.

195. CAs most commonly followed up on the breaches identified through orders to implement specific measures, orders to comply, warnings or fines. These measures appear to be in line with the level of seriousness of the breaches identified in the sector.

4.5.4 Emerging risks

196. As part of their identification of emerging risks, a number of CAs identified risks associated with investments offered in crypto-assets, which might be used in a fraud scheme. Some CAs raised concerns about investment firms registering as crypto-assets service providers as well, with no adequate AML framework.

197. FinTech and the greater role of technology in investment services is also a key risk in the sector where they are not implemented or monitored effectively. The increasing use of technologies in the sector may often cause challenges with the identification and verification of customers, and the monitoring of transactions, like peer-to-peer transactions.

198. The implementation of targeted financial sanctions by investment firms is considered by most CAs as a risk.

199. Some CAs indicated that trading with volatile stocks such as energy companies was an emerging money laundering risk.

Proposal: The EBA advises CAs to assess how to provide specific guidance to the sector to improve the sector's awareness of ML/TF risks and to ensure that supervisory expectations regarding adequate and effective AML/CFT systems and controls are well understood and applied. The EBA's Risk Factors Guidelines contain further details.

4.6 Collective investment undertakings

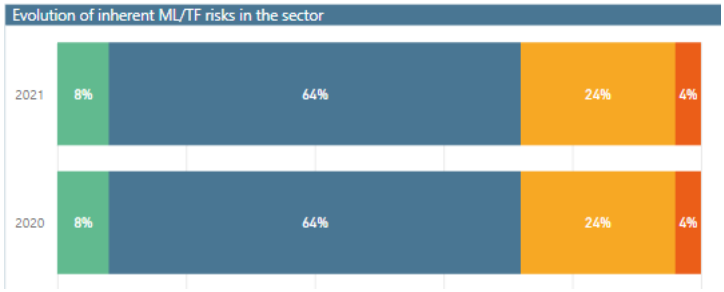
200. In total 25 CAs which are responsible for the AML/CFT supervision of 17 472 collective investment undertakings responded to the EBA's questionnaire in respect of data for both 2020 and 2021. The sector is highly concentrated, with 75% of the collective investment undertakings located in 2 Member States. This is the first time that the EBA distinguishes between supervisors of fund managers and those of collective investment undertakings, in line with supervisory practices.

201. Most CAs assessed the sector as presenting a moderate risk. A large number of CAs cited the sector's exposure to cross-border transactions as an area of concern. However, the intensity of supervisory activities appeared not to have been fully commensurate with the ML/TF risks.

4.6.1 Inherent risks

202. The sector is considered by 64% of CAs as presenting a moderate inherent risk.

Figure 44: Inherent ML/TF risks in the sector of collective investment undertakings



203. This is in spite of some CAs assessing the level of inherent risk associated with customers, delivery channels and geographies as very significant.

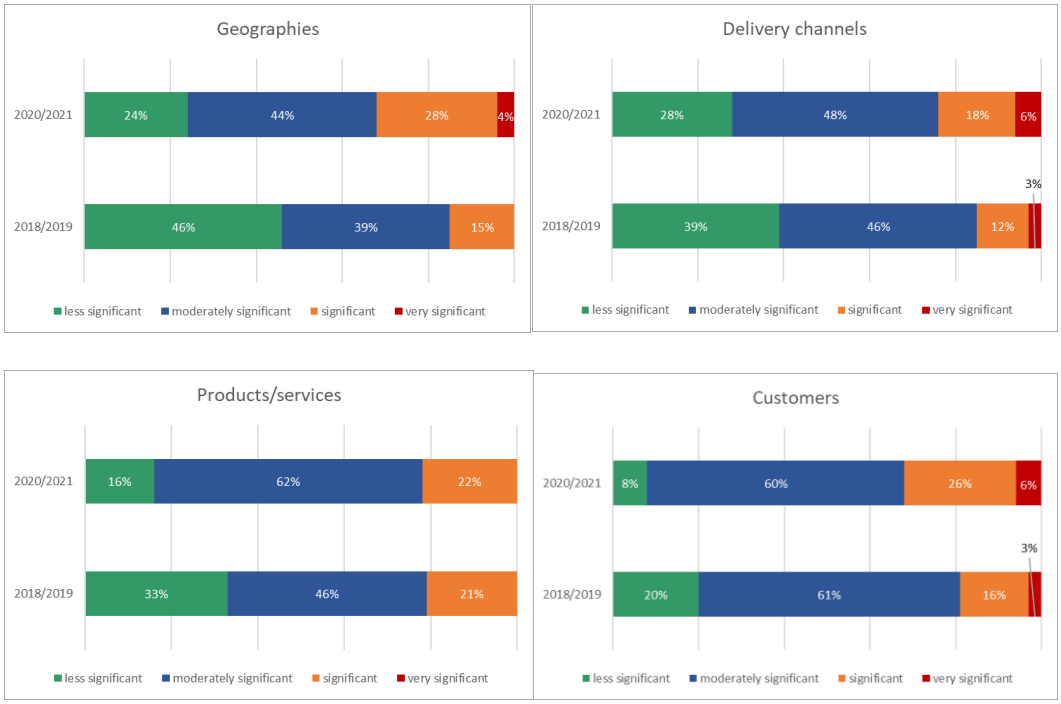
204. Most CAs consider customer and geographic risks to be key for the sector as a result of, for example, the prevalence in the sector of non-resident customers or customers located in higher risk jurisdictions: most CAs indicated that the exposure to UBOs from EU/EEA jurisdictions was moderately significant.

205. 24% of CAs assess risks associated with delivery channels as very high with a distribution of fund units through intermediaries, and the reliance on data provided by intermediaries. In some cases, depending on the set-up and the coverage of distribution of the fund, i.e. where these intermediaries are not themselves investors, i.e. owners, of the fund, this may lead to more lengthy identification processes, and especially in open-ended funds where no direct contact between the fund itself (but other service providers for the fund) and the investor is given. On the other hand, where intermediaries are the investors in the fund, specific rules and mitigation measures need to be applied to ensure that ultimate beneficial owners, where relevant, are identified.

206. The sector offers a wide variety of complex products, such as hedge funds, SICAVs, funds with international participations in other financial products – as unit-linked products, omnibus account services, marketing with entities with the freedom to provide services. Other risk products are private investor funds and private funds similar to asset protection vehicles. CAs indicated that some funds offer investments in high-risk sectors such as crypto-assets and real estate.

207. Other risks include tax evasion, even though the reporting level is low.

Figure 45: Inherent risk factors in the sector of collective investment undertakings



208. Inherent cross-border risks of delivery channels are rated by CAs as significant to very significant, followed by cross-border risks of customers.

4.6.2 Quality of controls and overall risk profile

209. The majority of CAs indicated that the data they provided for their assessment of the quality of controls put in place by firms in this sector was based on a formal risk assessment, such as the one envisaged in the EBA's Risk-based AML/CFT Supervision Guidelines. They rated the quality of controls as good overall in this sector though in around a quarter of all cases, those controls had not been assessed.

210. For example, 32% of CAs indicated they had not assessed either the adequacy or the effectiveness of governance structures in both 2020 and 2021. This is of concern, given that effective AML/CFT governance and oversight is an essential part of ML/TF risk mitigation and given that CAs noted the risk of conflict of interest with pressure to collect fees that might affect the use of sufficient AML/CFT controls.

211. Furthermore, approximately one quarter of CAs assessed the adequacy of STR policies and procedures, the effectiveness of ongoing monitoring and the effectiveness of STR reporting as poor or very poor in both 2020 and 2021.

Figure 46: Competent authorities' assessment of the quality of the controls in place in the sector of collective investment undertakings

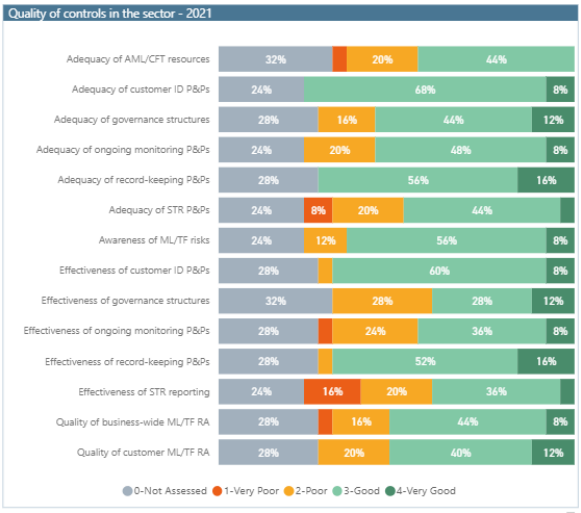
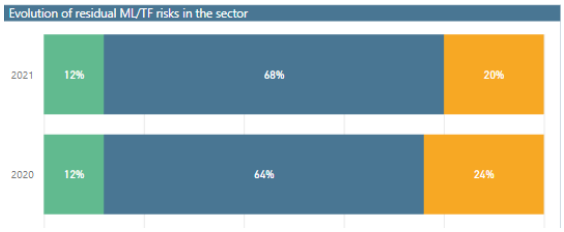


Figure 47: Evolution of residual risks in the sector of collective investment undertakings since 2020



4.6.3 Supervisory activities and breaches identified

212. Supervisory activity in the sector seems more limited in comparison with other sectors. The majority of on-site supervisory activities were scheduled inspections followed by other on-site engagements. However, on-site activities represented a very small proportion of the overall coverage of the sector in both 2020 and 2021. This may be because of the high number of firms in some jurisdictions, the risk rating CAs had given to the sector and the specific setups of the funds.

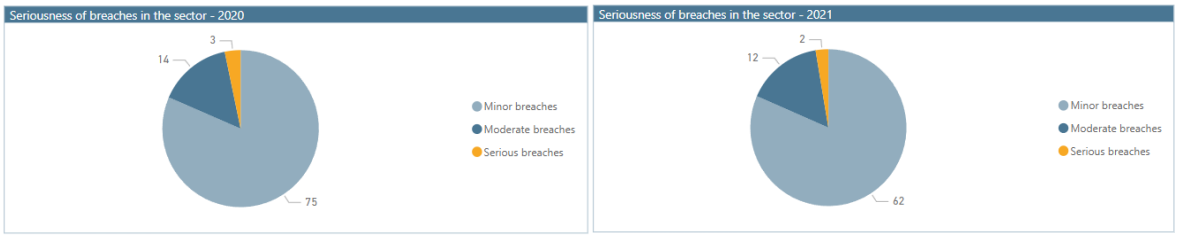
213. CAs indicated that the most common type of off-site supervisory activity conducted in the sector was through AML/CFT returns. Based on the ML/TF risk exposure of the sector, AML/CFT returns may be used by CAs to identify those firms that may be outliers in terms of their risk profile and that may warrant closer inspection.

Figure 48: Off-site and on-site inspections conducted in the sector of collective investment undertakings

214. From the information provided by CAs, the intensity of supervisory activities does not seem to have been fully commensurate with the ML/TF risk presented by firms in this sector. This may be explained partially because of the supervisory focus on investment fund managers and other intervening service providers instead of on the product itself.

215. CAs have identified a number of breaches. The vast majority of breaches were considered minor or moderate in nature for both 2020 and 2021. No egregious breaches were noted.

Figure 49: Seriousness of breaches identified in the sector of collective investment undertakings



216. The most common breaches identified in this sector related to internal controls and overall AML/CFT policies and procedures, ongoing monitoring, customer identification and verification, customers and business-wide risk assessment. This is very similar to the 2021 Opinion.

217. Feedback from CAs suggests that CAs have applied similar measures in case of identified breaches irrespective of the severity of the breach. These included requiring firms to comply or implement measures or impose a fine or sanction.

4.6.4 Emerging risks

218. Similar to other sectors, the most common emerging risk referenced by CAs in this sector related to risks associated with FinTech and Reg Tech solutions, in particular the increasing use of new technologies to identify and verify customers, as detailed in Section 3.2.3 where those are not implemented or monitored effectively.

219. Other emerging risks include investments in crypto-assets, which can prevent the identification of the selling party.

220. Many CAs referred to the risks related to sanctions breaches and circumvention of sanctions in the sector. From preliminary findings relative to the robustness of sanctions screening policies, procedures and controls, shortcomings were identified in some collective investment schemes.

221. Some CAs indicated a potential risk arising from the insufficient testing of new products. They noted that the diversification of assets invested in by collective investment schemes, which are becoming more illiquid and for which it is difficult to obtain valuation, may actually lead the sector to be more vulnerable to ML/FT.

Proposal: The EBA advises CAs 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.

4.7 Fund managers

222. In total 26 CAs responsible for the AML/CFT supervision of 5,705 fund managers responded to the EBA's questionnaire in respect of data for both 2020 and 2021. The sector is highly concentrated, with 65% of all fund managers located in 4 Member States. This is the first time that the risks associated with fund managers are assessed separately from collective investment undertakings.

223. Most CAs considered that fund managers had a moderately inherent risk profile. However the lack of systems and controls for identification and verification of beneficial ownership poses a significant to very significant risk according to most CAs.

4.7.1 Inherent risks

224. The medium to long-term nature of the investment strategy of many funds can limit the overall attractiveness of the sector for ML/TF purposes. This is why the sector is considered by most CAs as presenting a predominantly moderate and less significant risk from a ML/TF perspective.

Figure 50: Inherent ML/TF risks in the sector of fund managers

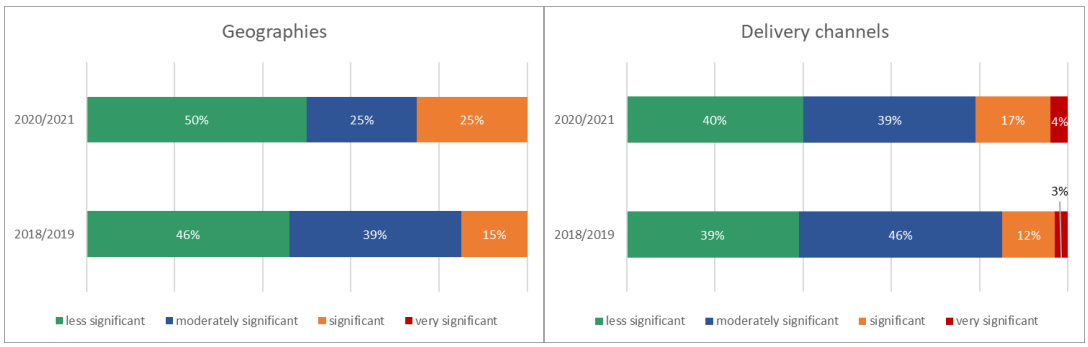
225. Risks associated with customers of the funds managed and delivery channel were considered by most CAs to be key for the sector as a result of the distribution of fund units through intermediaries, which makes the identification and management of ML/TF risk more challenging.

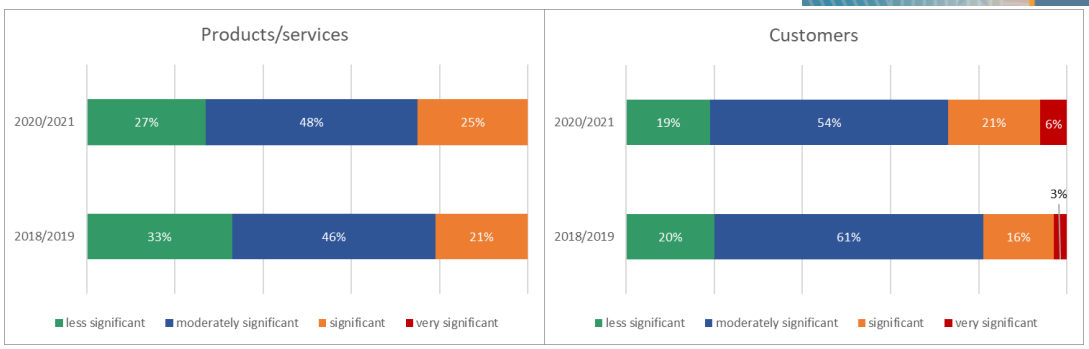
226. Risks related to customers of the fund managed are linked to the prevalence of high-net-worth individuals, customers with complex structures and non-resident customers, which are sometimes located in higher risk jurisdictions. Some CAs noted risks related to the link with citizenship and residence by investment schemes.

227. The sector may be abused to launder the proceeds resulting from criminal activity such as tax evasion, bribery, corruption and organised crime. CAs mentioned that some STRs from the sector reflect those trends, even if reporting rate remains low.

228. Some CAs indicated that investment in new asset classes such as crypto-assets is a current risk, while others view it as an emerging risk (see Section 4.11).

Figure 51: Inherent risk factors in the sector of fund managers





229. Inherent cross-border risks are mostly related to customers, at a significant level, with lesser risks associated with products/services and delivery channels.

4.7.2 Quality of controls and overall risk profile

230. Most CAs rated the quality of controls as good in this sector. They considered both the adequacy and effectiveness of policies and procedures that the sector had put in place to comply with their AML/CFT obligations to be good, but pointed to ongoing difficulties by firms in this sector in identifying PEPs or establishing the beneficial ownership of customers. CAs highlighted deficiencies linked to a lack of verification of source of wealth and source of funds, and of establishing the purpose and nature of the business relationship.

231. At the same time, around one third of CAs had not assessed either the adequacy or the effectiveness of governance structures. This is of concern, given that effective AML/CFT governance and oversight is an essential part of ML/TF risk mitigation and given the level of delegation in the sector. Some CAs noted the risks of conflict of interests that prevent an independent and adequate management of ML/TF risks related where investors are also shareholders or owners of investment products. Furthermore, fund management companies typically outsource AML/CFT activities to third party service providers which requires robust oversight and assurance testing programmes to be implemented.

232. Furthermore, around one third of CAs assessed the following controls as being poor in both 2020 and 2021: the adequacy of STR policies and procedures and the effectiveness of STR reporting, although ongoing monitoring was deemed adequate by 37% of all competent authorities. More than a quarter of CAs assessed the quality of business-wide risk assessments and individual risk assessment as poor. This appears to be in line with what was reported by CAs about the main customer risks in the sector.

233. After considering inherent risks and controls, most CAs assessed the overall residual ML/TF risk profile in the sector as moderately significant or less significant overall, though not all CAs had data available for 2021 yet and a quarter to a third of CAs had not assessed relevant controls in the sector in practice.

Figure 52: Competent authorities' assessment of the quality of the controls in place in the sector of fund managers

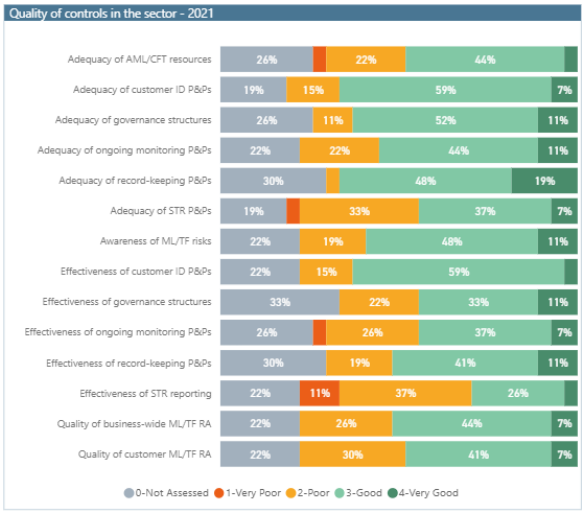


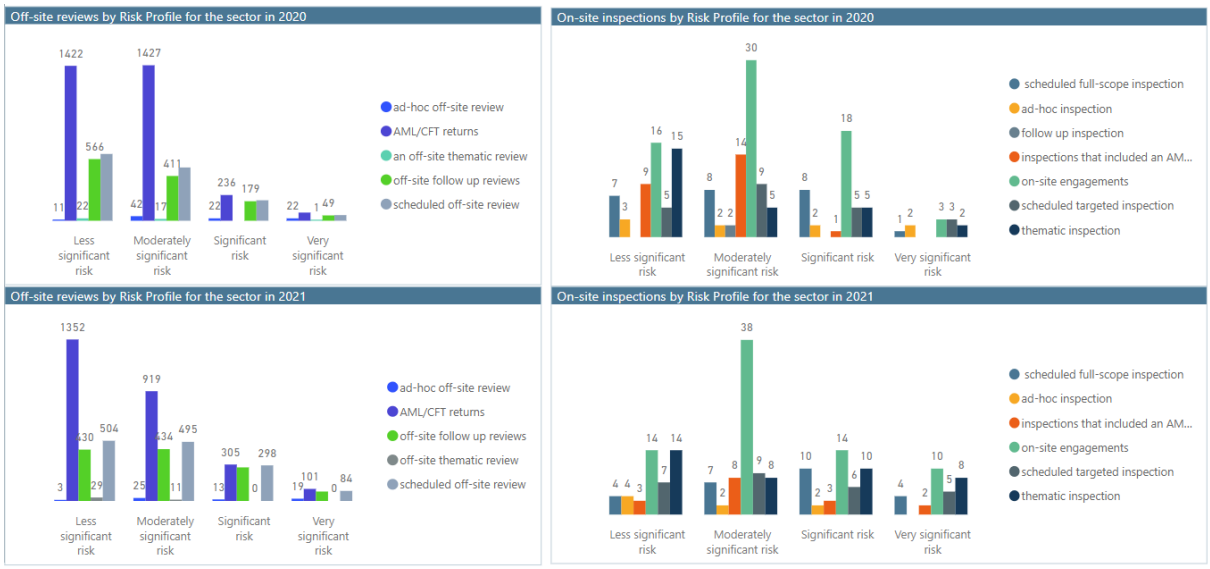
Figure 53: Evolution of inherent and residual risks since 2020 in the sector of fund managers

4.7.3 Supervisory activities and breaches identified

234. The sector received a lower level of on-site supervisory attention in comparison with other sectors. The majority of on-site supervisory activities were scheduled inspections followed by other on-site engagements. However, on-site activities represented a very small proportion of the overall coverage of the sector in both 2020 and 2021. Several CAs indicated that in 2020 they reduced the number of on-site inspections or postponed them due to the COVID-19 pandemic with a number of CAs carrying out their on-site activities remotely. In 2021, some CAs carried out hybrid inspections, but most CAs did not make any adjustments.

235. Most CAs indicated that the most common type of off-site supervisory activity conducted in the sector was through AML/CFT returns. Based on the ML/TF risk exposure of the sector, AML/CFT returns may be used by CAs to identify those firms that may be outliers in terms of their risk profile and that may warrant closer inspection.

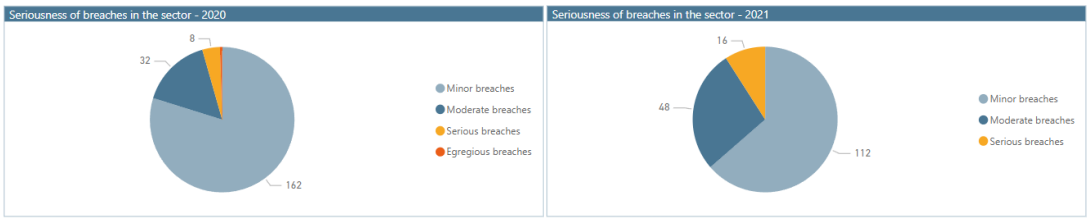
Figure 54: Off-site and on-site inspections conducted in the sector of fund managers



236. The information provided by some CAs suggests that the intensity of supervisory activities was not commensurate with the ML/TF risk presented by firms in this sector.

237. CAs identified a number of breaches during the reporting period. The vast majority of breaches were considered minor in nature for both 2020 and 2021. Almost no egregious breaches were noted in each year. This may be due to the limited supervisory activities in the sector. The number of breaches identified dropped in 2020 due to the decrease in supervisory activities with the COVID-19 pandemic. However, the number of breaches identified continued to slow down in 2021 as well.

Figure 55: Seriousness of breaches identified in the sector of fund managers



238. The most common breaches identified in this sector related to customer identification and verification, ongoing monitoring and internal controls and overall AML/CFT policies and procedures.

239. CAs required firms to comply, to implement measures or put in place a remediation plan for most identified breaches. Some fines were imposed irrespective of the severity of the breach for firms with an egregious breach, but also for serious and moderate breaches.

4.7.4 Emerging risks

240. Like other sectors, the most common emerging risk referenced by CAs in the sector related to risks associated with FinTech and Reg Tech solutions, in particular the increasing use of new technologies to identify and verify customers, as detailed in Section 3.2.3 where those solutions are not monitored or implemented efficiently.

241. Another emerging risk referenced by an increasing number of CAs compared to the 2021 Opinion is related to the sector offering higher risk assets such as crypto-assets.

242. Many CAs referred to the risks related to sanctions breaches and circumvention of sanctions in the sector.

Proposal: The EBA advises CAs to consider how best to address the identified weaknesses in controls, such as adequate oversight of AML/CFT framework put in place by fund managers as part of their supervisory approach.

4.8 Credit providers

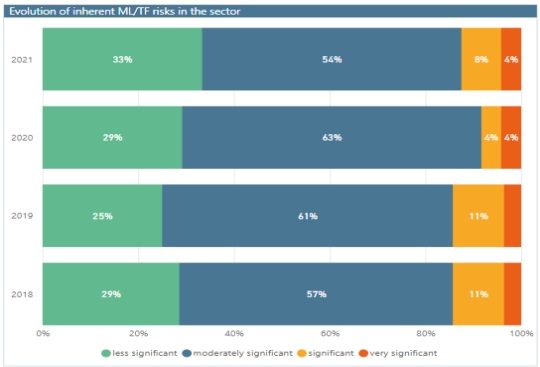
243. The EBA received responses from 25 CAs responsible for the AML/CFT supervision of 2 694 credit providers (CPs) in total for 2020 and 2021.

244. Most CAs considered the level of inherent risk in the sector to be moderately significant or less significant. The wide range of products and services of the sector offered through a variety of delivery channels lead to different types and levels of ML/TF risks. Almost all CAs indicated they performed an assessment on the quality of controls in the sector, which represents an improvement compared to the 2021 Opinion.

4.8.1 Inherent risks

245. Similar to the 2021 Opinion, most CAs considered the level of inherent risk in the sector to be moderately significant or less significant, with only a small number of CAs assessing the inherent ML/TF risk as significant or very significant. Almost all CAs that responded indicated that they provided this rating on the basis of a formal risk assessment, such as the one envisaged in the EBA's risk-based supervision guidelines, which represents a substantial improvement compared to the 2021 Opinion.

Figure 56: Inherent ML/TF risks in the sector of credit providers

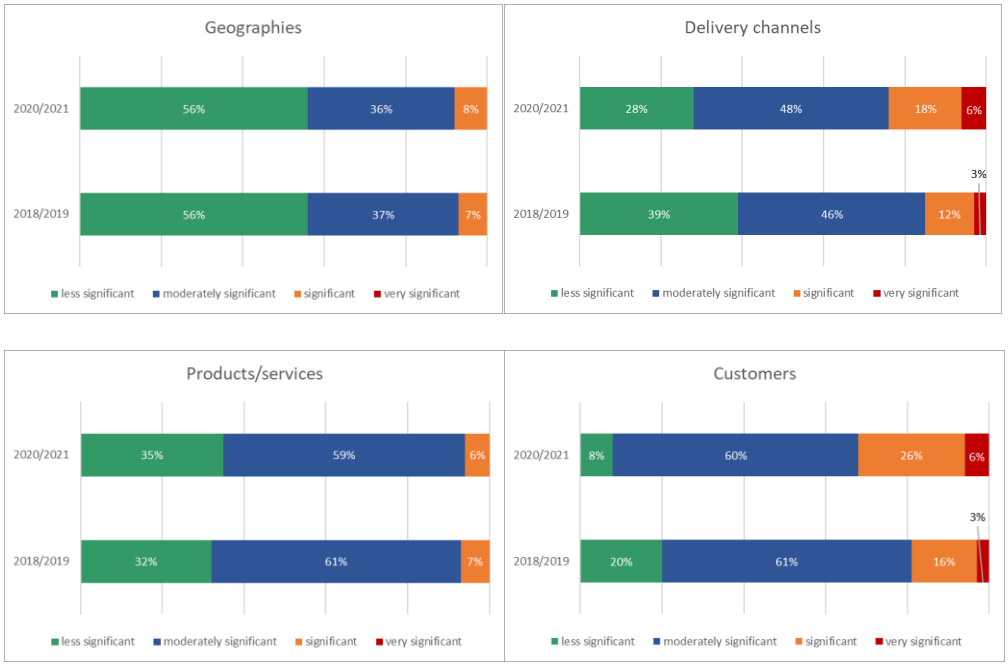


246. Firms in the sector are very diverse and may face different types and levels of ML/TF risks. Similar to the 2021 Opinion, CAs continued to note risks associated with the repayment of loan, either with money from criminal origins, against which the verification of source of funds is not robust, or with CPs accepting repayments from third parties instead of the end customer.

247. Factoring, leasing and commercial CPs serving customers like trading or import/export companies are more exposed to trade-based money laundering[67]. A few CAs noted occurrences where the leasing rate of some luxury goods was paid with the proceeds of crime.

248. CAs also noted that the sector was still vulnerable to being used for terrorist financing purposes as low-value loans, for which AML policies and procedures are often insufficient, can be obtained to finance terrorism.

Figure 57: Inherent ML/TF risk factors in the sector of credit providers



249. As the sector is mostly domestic in nature, most CAs considered the sector's cross-border risk exposure to present less or moderately significant risk. The small proportion of CAs that assessed geographical risks as very significant may be attributed to the exposure of some CPs to trade-based money laundering.

67 Trade finance products can be abused for money laundering and terrorist financing purposes, for example, the buyer and seller may collude to misrepresent the price, type, quality or quantity of goods in order to transfer funds or value between countries. See for more details in the revised EBA's risk factors guidelines, March 2021.

4.8.3 Quality of controls and overall risk profile

250. CAs consider the CPs sector to have moderately significant or less significant residual exposure to ML/TF risks, with very few CAs considering that the overall risk profile is significant or very significant. The rating of the overall residual risks in comparison to the overall inherent risk profile of the sector seems to indicate the controls in place are sufficient to mitigate the overall risk in the sector, although CAs' assessment of individual controls suggests that this is not the case.

251. More than 40% of CAs assessed the sector's awareness of ML/TF risks as poor. They also assessed the adequacy and effectiveness of policies and procedures for monitoring and suspicious transaction reporting as poor or very poor. The poor quality of these controls is particularly worrying in this sector in light of the inherent risks to which the sector is exposed.

252. For example, consumer CPs often operate through credit intermediaries, or non-face-to-face methods through online provision of services, which may result in less effective application of CDD measures. Some CAs indicated that when the market for consumer loans is highly competitive, there is a risk that sufficient CDD is not collected during the speedy approval process. Other risks related to CDD, which were already identified in the 2021 Opinion, are still current, with documentary fraud and identity theft to obtain consumer credits, and lack of verification of multiple loan applications across several credit providers.

Figure 58: Competent authorities' assessment of the quality of controls in place in the sector of credit providers

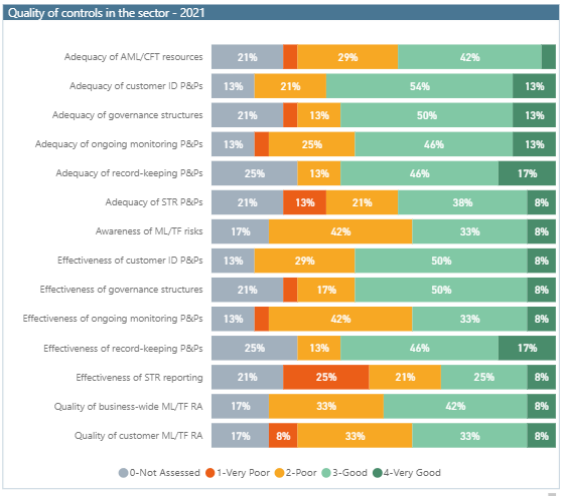
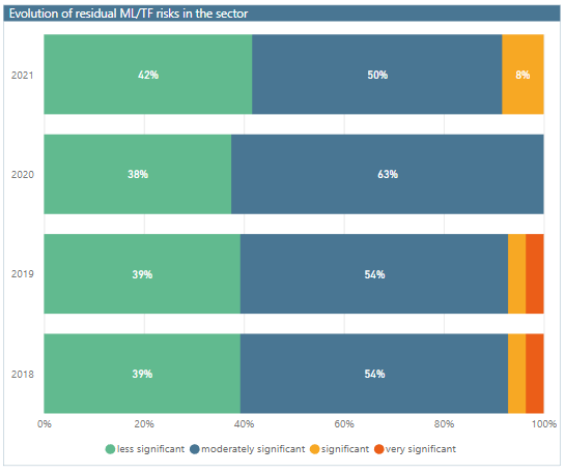


Figure 59: Evolution of residual risk profile of credit providers



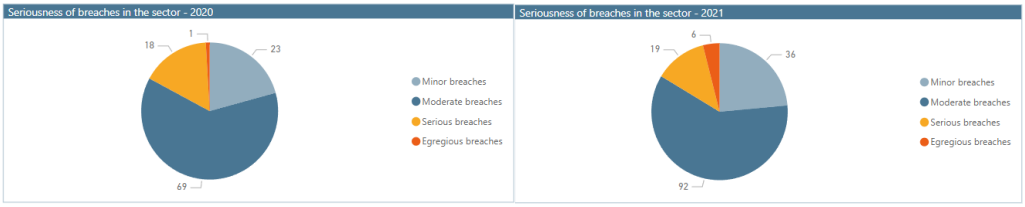
4.8.4 Supervisory activities and breaches identified

253. According to the information provided by CAs, the supervisory activities within the CPs sector were mostly conducted on an off-site basis and mainly through AML/CFT returns. Most CAs indicated that they had performed on-site inspections, but the large majority of on-site inspections in 2020 and 2021 were carried out by just one CA, on firms presenting a low risk profile.

Figure 60: Off-site and on-site inspections in the sector of credit providers

254. CAs identified a number of breaches. The vast majority of breaches were considered moderate in nature for both 2020 and 2021. Almost no egregious breaches were noted in each year. This may be due to a lack of focus of supervisory activities on credit providers of very significant risk. The number of breaches identified dropped in 2020 due to the decrease of supervisory activities with the COVID-19 pandemic.

Figure 61: Seriousness of breaches identified in the sector of credit providers



255. The most commonly identified breaches in the sector relate to the identification and verification of customers and customer risk assessments, overall AML/CFT policies and procedures and ongoing monitoring. This could be of concern in light of the risks to which the sector is exposed and considering that CPs' business model is generally based on processing large numbers of loans every day. Most of the breaches identified by the CAs were however rated as moderate.

256. The most common follow-up measures applied by CAs within the CPs sector are orders to comply and/or implement measures, followed by warning and administrative pecuniary sanctions, which appear to be commensurate with the seriousness of breaches (mostly moderate) identified by CAs.

4.8.5 Emerging risks

257. Feedback gathered from CAs indicated that the sector is exposed to risks resulting from overreliance on remote onboarding solution, without adequate safeguards to ensure the quality of these systems.

258. Several CAs raised concerns about an increase in mortgage lending by CPs with less robust AML/CFT framework than the retail banks from which they are taking those services. In particular, non-performing loan (NPL) credit servicing firms are expected to intensify their efforts in NPL management, which may increase repayment transactions from third parties (i.e. from real estate auctions or cross-border investors in companies). Furthermore, CAs noted risks related to the underlying assets of securitised non-performing loans, that could contain assets of companies related to organised crime.

259. Some CAs indicated that the current economic crisis could lead to an increase in the financing needs of the population that will not be absorbed by the credit institutions. Consequently, credit providers would absorb these clients, increasing the risk related to the volume of clients and type of operations.

Proposal: The EBA advises CAs to continue to identify the main risks in each subsector of credit providers and focus their supervisory activities on the areas which represent the highest ML/TF risk in this sector, such as non-performing loans management.

4.9 Life insurance undertakings

260. In total, 32 CAs responsible for the AML/CFT supervision of LIUs, responded to the EBA's questionnaire. Based on the information received from CAs, there are 955 LIUs that are supervised for AML/CFT compliance in the EU.

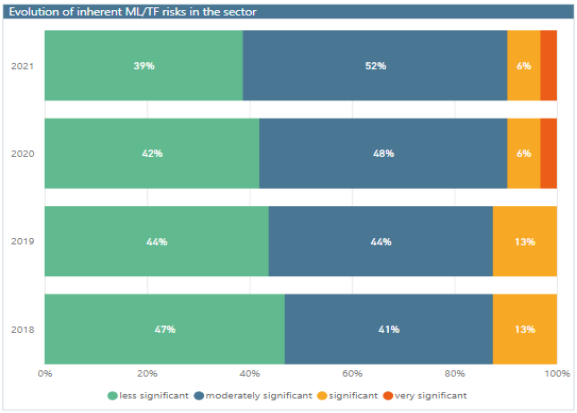
261. CAs considered the sector as presenting moderately significant or less significant risk from an inherent ML/TF risk perspective. A small proportion of CAs indicated that the sector presented significant risks. Almost all CAs indicated they performed an assessment of the quality of controls in the sector, which represents an improvement compared to the 2021 Opinion. A growing, significant proportion of CAs indicated that the sector's awareness of ML/TF risks has improved, however the effectiveness of suspicious transaction reporting remains a concern.

4.9.1 Inherent risks

262. Overall, the LIU sector is considered as presenting a moderately significant or less significant risk from an inherent ML/TF perspective by most CAs. Most CAs base their assessment of inherent risks of the sector on a formal risk assessment, such as the one envisaged in the EBA Risk-based Supervision Guidelines. One CA assessed the inherent risk level in the sector as very significant. Compared to the 2021 Opinion, nearly half of CAs consider the sector as presenting moderately significant risks, which represents an increase of 10%.

263. Nearly 40% of CAs considered the sector as presenting less significant exposure to ML/TF inherent risks. Similar to the 2021 Opinion, the sector has received low levels of supervisory activities and a large number of CAs responsible for the AML/CFT supervision of the sector indicated they did not carry out any supervisory activity in this sector.

Figure 62: Inherent ML/TF risk profile in the sector of life insurance undertakings



264. Like in the 2021 Opinion, distribution channels are considered to carry an increased level of risk. This is because of the higher prevalence in insurance than in other sectors of activities through insurance intermediaries.

265. Customers are increasingly considered to present higher risks compared to the 2021 Opinion, with an increase in moderately significant risks, and for the first time, a burgeoning level of significant risks. The main money laundering risks related to customers are by means of funding through or payment to third parties other than the policyholder, or payments to the customer's accounts abroad. Several CAs indicated an increase in the frequency of criminals, associates of criminals and PEPs in using insurance-based investment products.

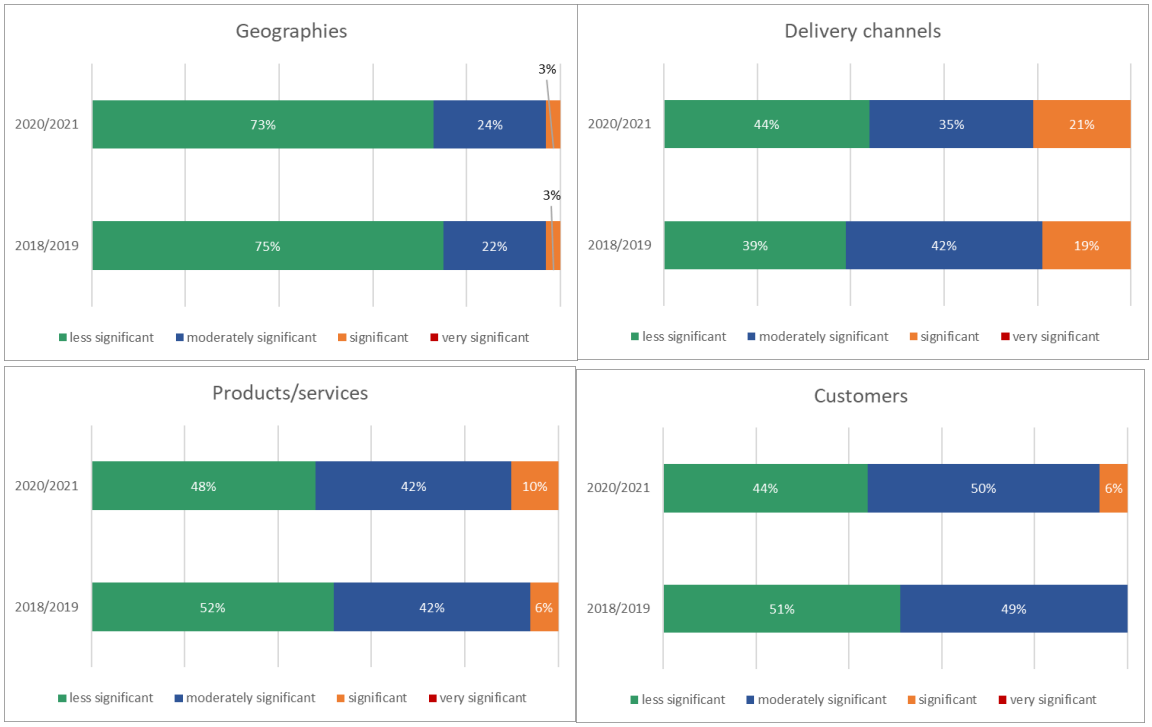
266. Tax-related crime is still considered an important threat to the life insurance sector, as not all life insurance companies have adequate controls such as the verification of origin of wealth and funds for the repatriation of capital and related income from abroad. CAs noted the misuse of life insurance contracts to avoid paying inheritance tax.

267. Products and services represent less significant to moderately significant level of risks, with a slight increase in the level of significant risks. The types of products and operations representing the main ML/TF risks are products with a short maturity period, like insurance-based investment products with a minimum holding period of 5 years, and those with the possibility of early termination of the policy.

268. Other products with higher ML/TF risks are investments associated with large life insurance policies. The most exposed insurance contracts, both single premium and regular premium, are unit-linked products with a high financial component and a low insurance component where the repayment of capital and interest is basically agreed. More flexible payment structures such as advance repayment, single payments of large denomination,

extraordinary payments of regular premium and diversification of payment structures can lead to increased risks.

Figure 63: Inherent ML/TF risk factors in the sector of life insurance undertakings



269. A large proportion of CAs assessed the sector's ML/TF risk exposure to cross-border transactions as less significant. The reason for this can be that cross-border business is mainly dealt with within the EEA countries.

4.9.2 Quality of controls and overall risk profile

270. The large majority of CAs have indicated that the data they provided for their assessment of the quality of controls put in place by firms was based on a formal risk assessment, such as the one envisaged in the Risk-based Supervision Guidelines.

271. Overall, most CAs that assessed the controls put in place by firms in the sector rated them as good. This result is similar to 2021 Opinion, and CAs appeared to be reasonably satisfied with the adequacy of controls related to the policies and procedures, particularly identification and verification of customers, record-keeping and ongoing monitoring, including transaction monitoring. Compared to the 2021 Opinion, CAs are less concerned about the effectiveness of those controls. However, several CAs indicated inadequate customer due diligence in relation to beneficial owners and PEPs.

272. The reduced effectiveness of suspicious transaction reporting remains a concern. This could be explained by the low frequency and or variability of the transactions compared to, for example, the banking sector. This however may be mitigated by the fact that the

transactions are mostly provided through bank accounts, which are generally covered by effective controls.

273. A significant proportion of CAs that has increased since the 2021 Opinion indicated that the sector's awareness of ML/TF risks have improved.

274. A significant part of CAs view the residual ML/TF risk profile in the sector as moderately significant or less significant. However, compared to the 2021 Opinion, an increasing number of firms are considered to have a significant risk profile or even a very significant risk profile. This may be due to the fact that most CAs carried out a formal risk assessment in 2020 and 2021 compared to the previous years.

Figure 64: Competent authorities' assessment of the quality of the controls in place in the sector of life insurance undertakings

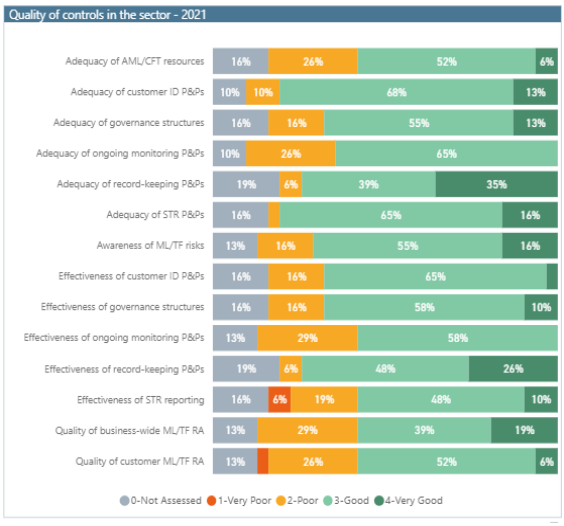
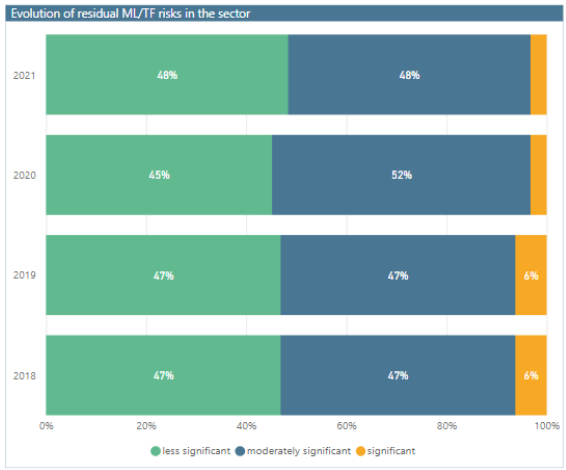


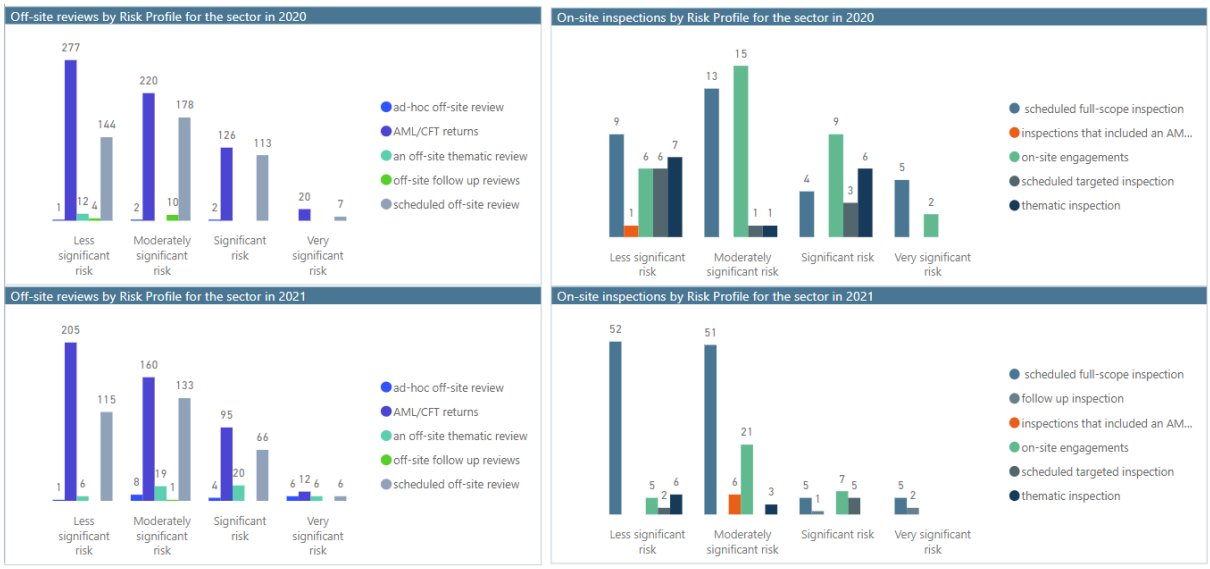
Figure 65: Evolution of residual ML/TF risks in the sector of life insurance undertakings since 2018



4.9.3 Supervisory activities and breaches identified

275. The sector is still subject to a relatively poor level of supervisory activity in comparison with other sectors. Not all CAs have conducted on-site or off-site inspections. If the number of on-site inspections decreased drastically compared to the 2021 Opinion, the number of off-site activities increased during 2020 and 2021. This may be attributed to a change in resources allocation and activities during the COVID-19 pandemic. Based on the responses received, the sector was mostly supervised through various off-site engagements, especially AML/CFT returns. CAs which also carried out on-site activities mainly carried out scheduled full-scope inspections.

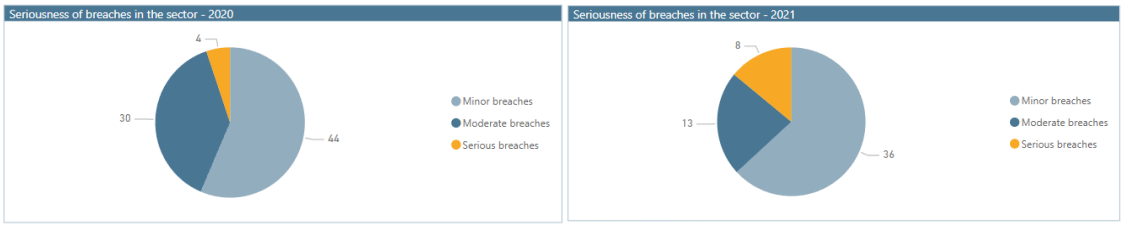
Figure 66: Off-site and on-site inspections in the sector of life insurance undertakings



276. The intensity of the supervisory activities appears to be commensurate with the ML/TF risk level CAs attributed to the firms in the sector. The majority of LIUs were associated with moderately significant or less significant risk profile. The volume of firms associated with a significant risk profile represented a small proportion and were mostly identified in jurisdictions in which the LIUs sector is more significant.

277. As a result of their supervisory activities, CAs identified some breaches in the sector that are considered minor or moderate, with an increase in serious breaches, mainly resulting from targeted and thematic inspections carried out by 1 CA. The total number of breaches, however, decreased substantially compared to the 2021 Opinion, as a result of a drop in supervisory activities in 2020.

Figure 67: Seriousness of the breaches identified in the sector of life insurance undertakings



278. The type of breaches that were identified by CAs as a result of their supervisory activities were mainly linked to customers' identification and verification, internal controls and overall AML/CFT policies and procedures, and ongoing monitoring including transaction monitoring. Breaches found in the sector are therefore rather in line with the assessment of the quality of controls.

279. Feedback from CAs suggested the most common follow-up measures were warnings, orders to implement measures, and orders to comply, in line with the seriousness of breaches

(mostly minor or moderate) identified by CAs in this sector. Fines were given by 1 CA which identified the most serious breaches.

4.9.4 Emerging risks

280. According to CAs, the increased use of FinTech and RegTech solutions in the sector appears to be a key emerging risk when appropriate monitoring controls are not in place. CAs are also concerned about the rise of web-based insurance platforms using 'Insurtech' and challenges posed by accounts opened without the physical presence of the customer and remote business relationships.

281. Traditionally, insurance products have not been frequently hired online. Nevertheless, an increase has been observed in clients operating remotely from other countries after the COVID-19 pandemic and the expansion of non-face-to-face services.

282. One CA mentioned the exploration by some cross-border life insurance companies of the provision of fly-to-buy life insurance products for non-EEA nationals.

283. Another CA identified the emerging trend of acquisition of existing life insurance portfolios from other firms, becoming a part of the strategy of some life insurance companies to further expand their business. At the same time, it is observed that the management of these portfolios is often outsourced, which exposes the owner/acquirer to significant outsourcings risks. Whilst the acquirer remains of course ultimately responsible for keeping the ML/TF risks arising from these portfolios under control, the extensive outsourcing in combination with such patchwork of portfolios might hamper the adoption of a harmonised and coordinated AML approach by these institutions.

284. Finally, 1 CA noted a recent increase in single-premium contracts with transactions higher than 1 million euros.

Proposal: The EBA advises CAs to consider how best to address the identified weaknesses in controls, such as customer identification and verification, in relation to beneficial owners and PEPs, put in place by life insurance undertakings as part of their supervisory approach.

4.10 Life insurance intermediaries

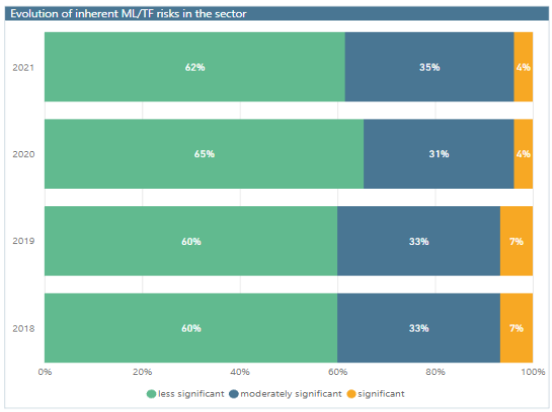
285. In total, 25 CAs, which are responsible for the AML/CFT supervision of 58 193 LIIs, responded to the EBAs' questionnaire and provided data for both 2020 and 2021. The number of LIIs supervised by the respondent AML/CFT supervisors represent only a fraction of the 815

219 registered insurance intermediaries operating at the end of 2020, according to the EIOPA's report on the application of the Insurance Distribution Directive[68].

4.10.1 Inherent risks

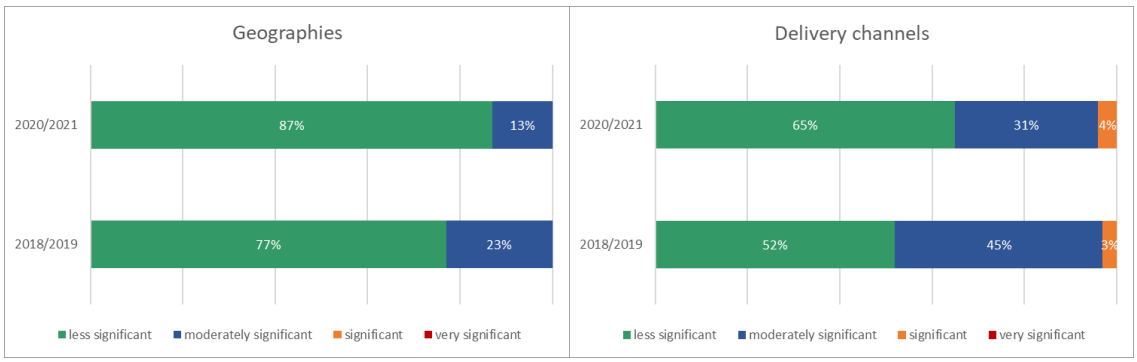
286. Most CAs considered the LII sector's exposure to ML/TF risks to be less significant.

Figure 68: Inherent ML/TF risks in the sector of life insurance intermediaries

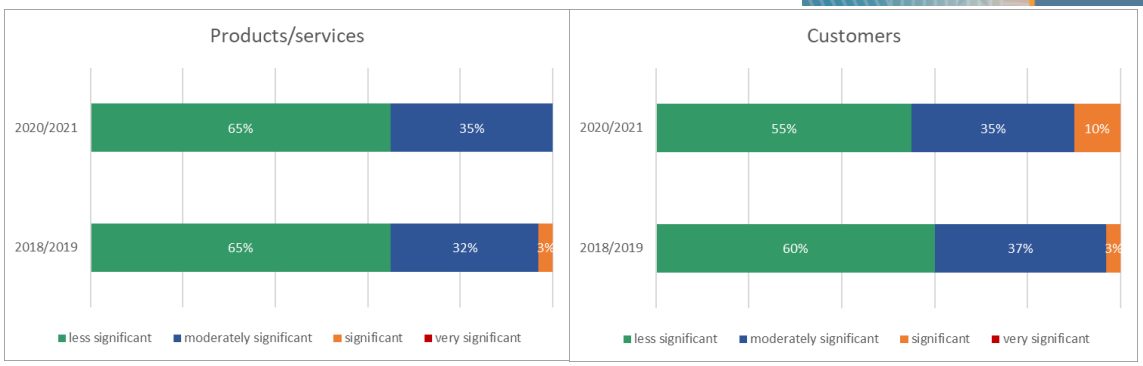


287. A large proportion of CAs assessed the inherent risks factors linked to geographies, and products/services as less significant in the sector of LIIs. Compared to the 2021 Opinion, many CAs considered that risks factors related to geographies decreased. Customers and distribution channels were rated as moderately significant by more CAs, but the proportion slightly decreased compared to the 2021 Opinion.

Figure 69: Inherent ML/TF risk factors in the sector of life insurance intermediaries



68 Report on the application of the Insurance Distribution Directive (IDD) (europa.eu)



288. CAs indicated that life insurance intermediaries sell less high-risk products than life insurance undertakings. However, many CAs noted risks related to tax-related crimes, with or without collusion with customers. As for life insurance undertakings, early repurchase brings a higher risk of ML, especially when carried out by a newly designated beneficiary or from an unknown bank account.

289. The sector's exposure to ML/TF risks related to cross-border transactions was also considered less significant by most CAs.

4.10.2 Quality of controls and overall risk profile

290. Compared to the 2021 Opinion, the large majority of CAs have carried out an assessment of controls. They considered that the controls put in place by LIIs were good or very good overall.

291. Generally, CAs appeared to be satisfied with the controls relating to the adequacy and effectiveness of customer identification and verification policies and procedures, as well as the adequacy and effectiveness of record-keeping policies and procedures. However, they appeared to be more concerned about the controls relating to the adequacy and effectiveness of STR policies and procedures, the quality of both the business-wide and individual risk assessments and the awareness of ML/TF risks. The latter raises questions about the effectiveness of CDD measures. Moreover, a significant number of CAs pointed to problems associated with the level of training provided to the staff in the sector, which was considered inadequate, notwithstanding the fact that there is an existing requirement under the Insurance Distribution Directive (IDD) for insurance intermediaries to have appropriate knowledge of anti-money laundering legislation[69].

292. Several CAs reported that a sales-oriented focus combined with elements of commission within the sector can lead to conflicts of interest between customer retention and CDD obligations, leading to incomplete CDD.

69 See Article 10, IDD and Annex I of the IDD

293. Some CAs noted insufficient AML/CFT governance, as most entities in the sector are small operations, sometimes even run by one or a few individuals. With a limited number of individuals, the AML/CFT governance may be limited in scope.

294. As in the 2021 Opinion, after considering inherent risks and controls, the majority of CAs view the overall ML/TF risk profile in the sector as less significant.

295. The overall residual risk profile of this sector remains broadly the same since the 2021 Opinion. The proportion of firms with a moderately significant profile however slightly increased.

Figure 70: Competent authorities' assessment of the quality of the controls in place in the sector of life insurance intermediaries

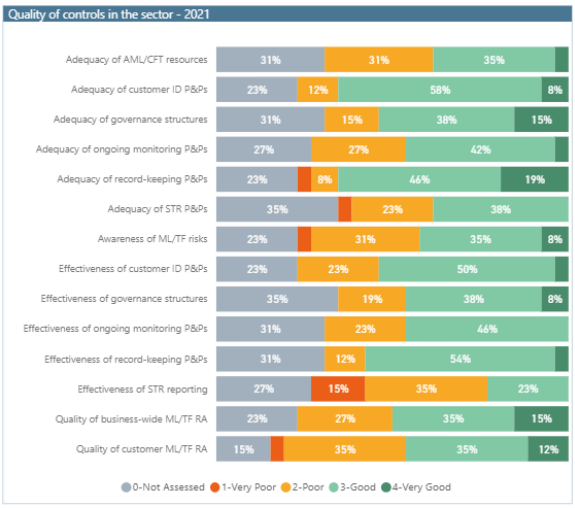
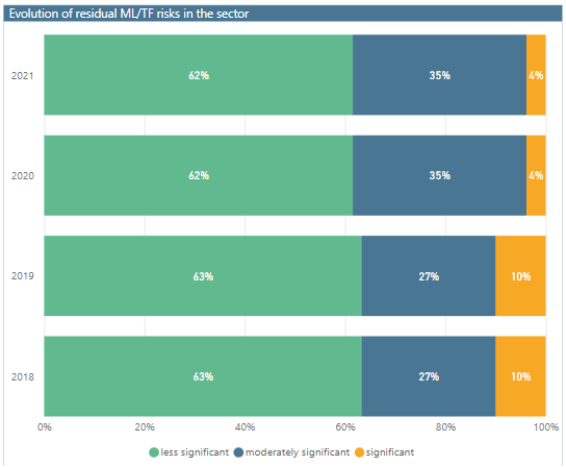


Figure 71: Evolution of residual ML/TF risk profile in the sector of the life insurance intermediaries since 2018

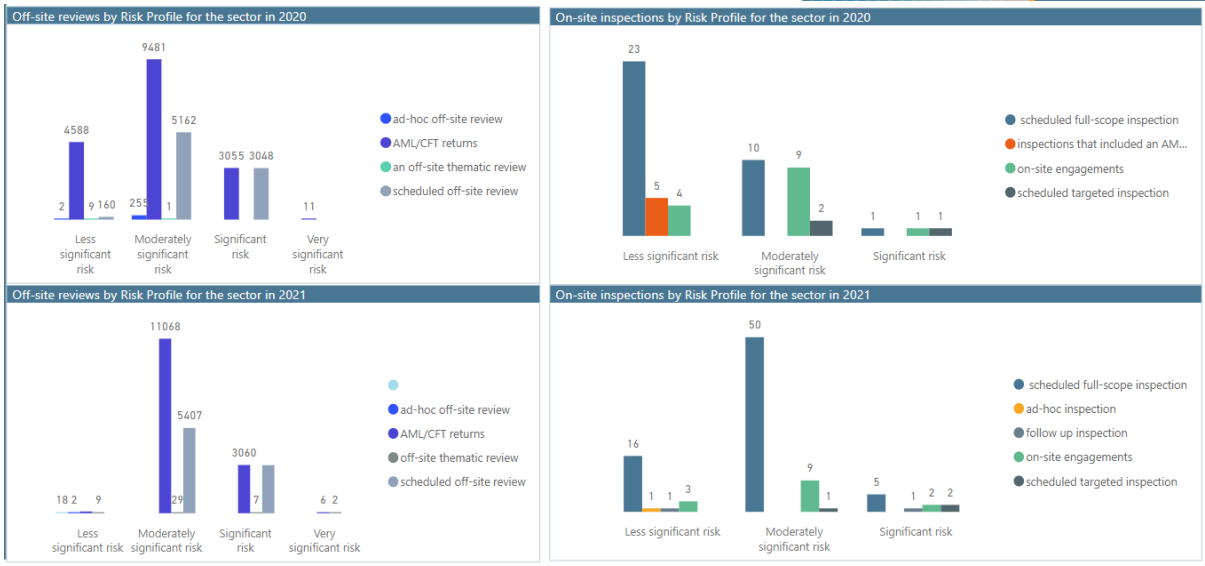


4.10.3 Supervisory activities and breaches identified

296. Similar to the 2018-2019 period reviewed in the 2021 Opinion, more than half of the CAs responsible for the AML/CFT supervision of LIIs did not carry out any supervisory activity in this sector in 2020 and 2021, and the sector has been subject to low levels of supervisory activities.

297. When CAs carried out on-site inspections, most of these were full-scope inspections. Despite adjustments in the way the on-site inspections were carried out during the COVID-19 pandemic, the total number of on-site inspections dropped in 2020. In 2021 1 CA accounted for almost half of the on-site inspections. For off-site activities, CAs mainly used AML/CFT returns.

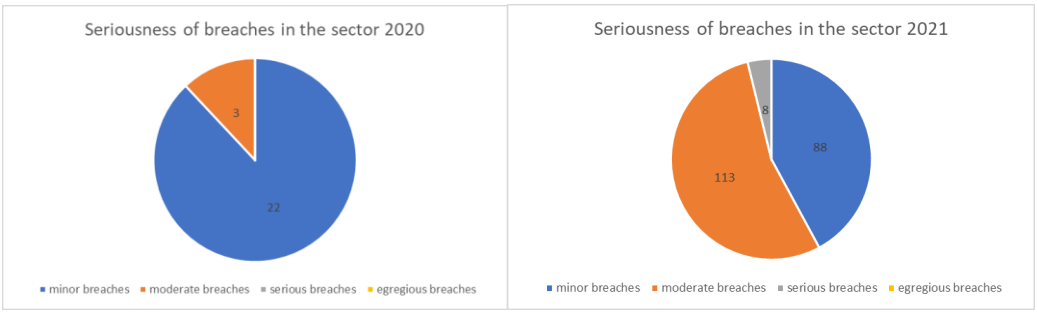
Figure 72: Off-site and on-site inspections carried out in the sector of life insurance intermediaries



298. There was some evidence from questionnaire responses that CAs followed a risk-based approach, commensurate with the number of firms in these risk categories. There was also significant supervisory activity with regard to lower-risk firms that CAs approached mainly through questionnaires/AML returns.

299. CAs identified a small number of breaches in the sector that were mainly classified as minor or moderate. The increased number of moderate breaches between 2020 and 2021 is a result of a drop in inspections carried out by CAs during the COVID-19 pandemic in 2020, and the fact that 1 CA carried out a large number of on-site inspections which accounted for almost half of the total number of on-site inspections.

Figure 73: Seriousness of the breaches identified in the sector of life insurance intermediaries



300. From the responses received, it appears that the main breaches were related to the internal controls and overall AML/CFT policies and procedures, identification and verification of the identity of customers, and ongoing monitoring, including transaction monitoring.

301. The most common follow-up measures applied by CAs to LIIs were warnings, followed by orders to comply and administrative pecuniary sanctions, which is in line with the seriousness of breaches identified.

4.10.4 Emerging risks

302. The majority of CAs identified the changes in the distribution channels used by LIIs as an emerging risk due to the increased use of FinTech that include InsurTech solutions. These new remote business relationships are an increasing risk factor while often inadequate CDD measures are already applied by LIIs.

303. One CA has experienced an increase in entities that issue corporate bonds abroad, before being distributed in the national market. This practice might lead to increased risks related to traceability of funds.

304. Several CAs mentioned the risk of non-compliance of LIIs with the increasing number of restrictive measures.

4.11 Crypto-assets service providers

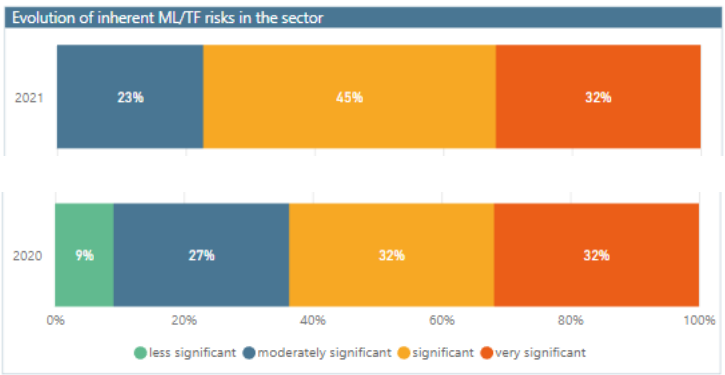
305. In total, 21 CAs, which are responsible for the AML/CFT supervision of 976 obliged entities that are CASPs, responded to the EBA's questionnaire in respect of data for both 2020 and 2021.

306. Assessed for the first time for the EBA's Opinion on ML/TF risks, CAs considered the sector to pose significant to very significant inherent ML/TF risks, identified through an increasing number of formal risk assessments. Many CAs did not assess controls of CASPs due to their recent inclusion as supervised entities. However most breaches identified in the sector related to customer identification and verification, internal controls and overall AML/CFT procedures, including customer risk assessment and transaction monitoring.

4.11.1 Inherent risks

307. CAs considered that the sector of CASPs poses mostly significant or very significant inherent ML/TF risks. The number of CAs that consider the sector to pose significant risks increased between 2020 and 2021 (from 29% in 2020 to 43% in 2021) due to more formal risk assessments carried out by competent authorities.

Figure 74: Inherent ML/TF risks in the sector of crypto-assets service providers



308. This assessment is mirrored in the ratings given by CAs to each risk factor, with products and services and delivery channels representing very significant risks. Customers pose significant risk and geographies only a moderately significant risk.

Figure 75: Inherent ML/TF risk factors in the sector of crypto-asset service providers

309. Main inherent risks identified are the pseudo-anonymity of transactions, the interaction with the dark web, the use of crypto-assets in predicate offences such as cybercrime, complex fraud schemes, crypto-investment scams[70], increasing money laundering[71], circumvention of sanctions. Some CAs highlighted risks in relation to the lack of cooperation between banks and CASPs, while others mentioned transfers from supervised CASPs to unsupervised CASPs. Crypto-assets services providers are used to collecting funds for terrorist financing purposes, and in some combat zones. Their actual use is not widespread because of limited liquidity and market penetration.

310. Inherent cross-border risks related to products and services of CASPs are very significant, while customers and geographies pose significant risks. CAs underlined that international or non-resident customers pose a risk, due to the global reach of CASPs.

4.11.2 Quality of controls and overall risk profile

70 Europol, Crypto investment scams – infographic

71 Europol, Cryptocurrencies: tracing the evolution of criminal finances

311. Two third of CAs indicated that the data they provided for their assessment of the quality of controls put in place by firms was based on a formal risk assessment as envisaged in the EBA's risk-based supervision guidelines.

312. Many CAs did not assess controls of CASPs in 2020 due to their recent inclusion as supervised entities. Overall, in 2020, CAs that carried out an assessment assessed most controls as either poor or good. In 2021, a number of controls were rated positively by most CAs. CAs identified a recurrent lack of appropriate CDD. In some cases, no CDD is carried out, such as crypto-ATMs, or transactions between individual traders on major exchange platforms. The frequent lack of identification of the beneficial owner and PEPs, as well as the insufficient risk assessment, prevent the relevant EDD from being carried out.

313. Beyond CDD deficiencies, the lack of adequate policies and procedures by CASPs is a significant risk, especially regarding transaction monitoring, as is the lack of AML/CFT training and awareness which is important to understand the ML/TF risks. Another risk is the reliance of CASPs on the same analysis tools that are not always updated or accurate, like clustering analysis for exchangers.

314. Most CAs viewed the overall residual ML/TF risk profile in the sector as significant. Significant residual risks have increased between 2020 and 2021, although this could be due to more CAs assessing and supervising the sector with a more accurate perception of the sector.

Figure 76: Competent authorities' assessment of the quality of controls in place in the sector of crypto-assets service providers

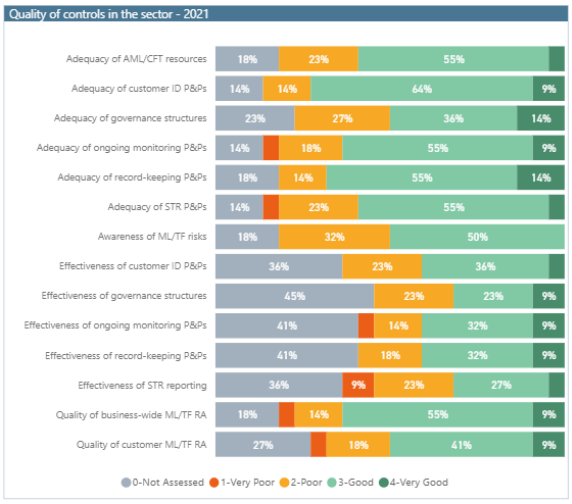
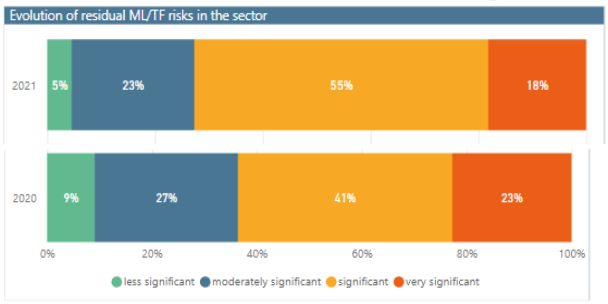


Figure 77: Evolution of residual ML/TF risks in the sector of crypto-assets service providers



4.11.3 Supervisory activities and breaches identified

315. As a recently supervised sector, only 7 CAs carried out on-site inspections in 2020, with 1 CA carrying out more than half of the 75 on-site inspections that year. Eleven CAs carried out on-site inspections in 2021, with 43 % of them by 1 CA. Most were full-scope inspections, followed by on-site engagements.

316. Eight CAs carried out off-site activities in 2020, while 11 CAs did so in 2021, mainly through AML/CFT returns and scheduled reviews.

317. Very few CAs had supervisory activities planned for CASPs in 2020 and 2021, so the COVID-19 pandemic did not bring many changes. CAs that had some inspections used remote-tools like direct IT access into institution´s core systems, data-uploads into secure file sharing platforms and video interviews. CAs indicated permanent changes to their

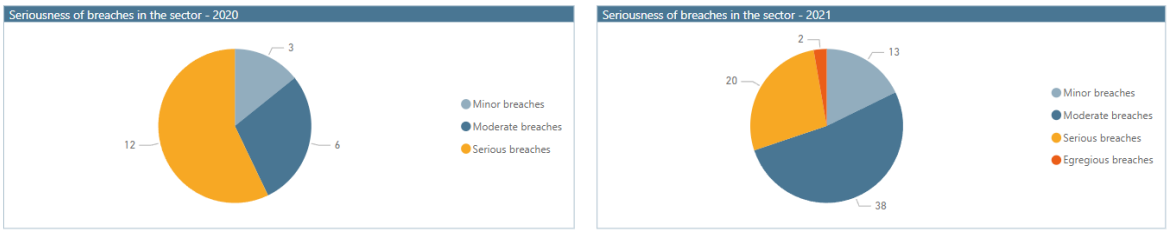
supervision brought by the COVID-19 pandemic: changes to on-site inspections with more use of remote tools, and more in-depth off-site examinations.

Figure 78: Off-site and on-site inspections in the sector of crypto-assets service providers

318. The information provided by CAs suggests that where inspections took place, they were broadly in line with the ML/TF risks presented by firms in the sector. Firms with a very significant risk profile were subject to the majority of supervisory activities, both off-site and on-site.

319. CAs identified only a small number of breaches, with more breaches identified in 2021. The vast majority of breaches were considered serious or moderate in nature for both 2020 and 2021.

Figure 79: Seriousness of breaches identified in the sector of crypto-assets service providers



320. Most breaches in the sector related to customer identification and verification of ID, internal controls and overall AML/CFT policies and procedures, transaction monitoring and customer risk assessment. This is broadly in line with the quality of controls about which CAs were generally concerned in the sector.

321. Feedback from CAs suggests that the most common supervisory measures used across CAs to mitigate weaknesses in firms' AML/CFT systems and controls included orders to comply or to implement measures and warnings. Six fines or pecuniary sanctions were imposed. However, in 4 cases with breaches identified as egregious or serious, the CAs applied a full withdrawal of authorisation or a deregistration of the entity.

4.11.4 Emerging risks

322. New risks are emerging in relation to new products such as non-fungible tokens, and more and more varied business models of CASPs, offering products with a higher level of complexity. The lack of consumer awareness has increased the amount of fraud carried out with crypto-assets. This might increase the financial stability risks in the future. Many CAs emphasised their lack of experience with new products such as DeFi and smart contracts. CAs also feel burdened by the increased number of applicants, coming from big companies with many subsidiaries, offering complex products. Many new entrants lack of robust AML knowledge. The use of automated on-boarding solution with insufficient safeguards, as well as the transfer of responsibility for KYC when e-money institutions operate as a distribution channel for CASPs are emerging risks in relation to already poor CDD.

Proposals: The EBA advises CAs to ensure that their staff receive the adequate and up-to-date training to have the technical skills and expertise necessary for the execution of their functions.

The EBA advises CAs to focus their risk assessment on areas identified in the forthcoming amendments to the EBA's Risk Factors Guidelines and the amendments to the Guidelines to prevent the abuse of fund transfers for ML/TF purposes.

4.12 Other financial sectors

323. 14 CAs from 10 Member States indicated they also supervise other financial sectors, as follows:

324. Regarding financial markets:

- central securities depository, custodian: 4 CAs;
- market operator: 1 CA;
- credit securitisation companies/ regulated securitisation vehicles: 2 CAs;
- venture capital companies, entities managing or marketing venture capital funds: 1 CA.

325. Regarding the insurance sector:

- pension insurance companies/pension funds/ foreign institutions of occupational retirement: 4 CAs;

- non-life insurance and reinsurance undertaking, non-life insurance undertakings, non-life insurance intermediaries: 2 CAs;

- mutual guarantee institutions: 1 CA.

326. Regarding crowdfunding services, 4 CAs supervise crowdfunding and peer-to-peer lending platform operators, crowdfunding platforms (donations, not-for-profit lending), or crowdfunding investment advisers.

327. One CA indicated they already supervise public offering of crypto-assets.

328. One CA supervises postal services, with financial products on their own account. Two CAs supervise credit intermediaries or banking brokers.

329. Those sectors are rather limited in size compared to other sectors. For the large majority of CAs, those sectors pose less significant or moderately significant inherent risks. The current risks identified are similar to other sectors such as lack of proper identification of customers and beneficial owners, especially in the context of remote on-boarding. Some products have potential customers from third countries that could higher-risk countries. Emerging risks are similar to other sectors, such as the risk related to the implementation of restrictive measures and the use of FinTech with inadequate safeguards.

330. The supervisory activities in relation to those sectors is in line with their risk profile. Some full-scope inspections were carried out for financial institutions with a very significant or significant risk profile, while CAs opted for on-site engagements for most other risk categories. CAs favoured scheduled off-site reviews and AML/CFT returns as off-site supervisory activities.

331. CAs mostly identified minor and moderate breaches and no egregious breaches were identified in 2020 and 2021. Measures were mostly orders to comply or to implement measures, and a few fines/administrative pecuniary sanctions.

Annex 1: Terminology

For the purpose of the EBA's questionnaire to CAs, the following terminology applied:

Scheduled full-scope inspection	means a comprehensive on-site review of all AML/CFT systems and controls implemented by subjects of assessment or their business lines, which takes place on the premises of subject of assessment and is scheduled in line with the risk-based approach. This assessment is likely to include a review of the firm's policies and procedures and an assessment of their implementation through, *inter alia*, interviews with key personnel, testing of systems used in the AML/CFT compliance and a review of risk assessment and customer files.
Scheduled targeted inspection	means an on-site review that focuses on one or more specific aspects of a subject of assessment's AML/CFT systems and controls framework. Such a review is scheduled in line with the risk-based approach. This assessment is likely to include a review of the subject of assessment's policies and procedures and an assessment of their implementation in respect of the targeted areas for review through, *inter alia*, interviews with key personnel, testing of systems used in the AML/CFT compliance and a review of risk assessment and customer files.
On-site thematic inspection	means on-site review of a number of subjects of assessment, often from the same sector, that focus on one specific or very few aspects of these subjects of assessments' AML/CFT systems and controls, such as transaction monitoring or the treatment of PEPs. Thematic reviews often serve to help supervisors gain a better understanding of the way specific ML/TF risks are managed by a sector, or particular types of credit and financial institutions.
Ad hoc on-site inspection	means an on-site review, whether comprehensive or focusing on a particular aspect of a subject of assessment's AML/CFT policies and procedures, that is triggered by a specific event such as whistleblowing, public allegations of wrongdoing (such as the Panama papers), or ML/TF risk, such as a new ML/TF typology or findings from another supervisory action such as an assessment of wider internal controls, or findings from an AML/CFT questionnaire.

On-site follow-up inspection	means an on-site review, which is consequent to a scheduled, an ad hoc or thematic inspection/review, and focusses on assessing whether weaknesses in a subject of assessment's AML/CFT systems and controls framework identified during a previous inspection or review have been corrected. This assessment is likely to include a review of the subject of assessment's written policies and procedures and an assessment of their implementation through, *inter alia*, interviews with key personnel, testing of relevant systems used in the AML/ CFT compliance and a review of risk assessment and customer files.
On-site inspection with an AML/CFT element	means an on-site review of a subject of assessment's overall systems and controls framework, which may be scheduled or ad hoc, where the assessment of AML/CFT systems and controls is not the main focus of the assessment, but form part of it. For example, where the main focus of the assessment is on the subject of assessment's compliance with prudential requirements and performed by prudential supervisors in conjunction with AML/CFT supervisors that are responsible for the assessment of AML/CFT systems and controls. This assessment is likely to include a review of the subject of assessment's policies and procedures and an assessment of their implementation through *inter alia* interviews with key personnel, testing of systems used in the AML/ CFT compliance and a review of risk assessment and customer files.
On-site engagements	means other types of on-site engagements with a subject of assessment or the subject of assessment's key personnel either at the premises of the firm or at the competent authority. Such an engagement is not part of the other type of on-site inspection. These engagements are likely to include bi-lateral meetings with the subject of assessment's personnel, which are scheduled in line with the risk-based approach.
Scheduled off-site review	means a comprehensive / full scope off-site review of a subject of assessment's AML/CFT systems and controls on the basis of written policies and procedures and risk assessments. Off-site reviews are scheduled in line with the risk-based approach and do not normally involve testing the implementation of these policies and procedures. Off-site reviews do not take place on the premises of subjects of assessment.
Ad hoc off-site review	means an off-site review, whether comprehensive or focusing on a particular aspect of a subject of assessment's AML/CFT policies and

	procedures, that is triggered by a specific event, such as whistleblowing, public allegations of wrongdoing (such as the Panama papers), or ML/TF risk, such as a new ML/TF typology or findings from another supervisory action such as an assessment of wider internal controls, or findings from an AML/CFT questionnaire. Off-site reviews do not take place on the premises of subjects of assessment.
Off-site follow-up review	means an off-site review, which is consequent to a scheduled or an ad hoc off-site review and focusses on assessing whether weaknesses in subject of assessment's AML/CFT systems and controls framework identified during the scheduled/ ad hoc inspection have been mitigated. This assessment is likely to include a review of a subject of assessment's AML/CFT systems and controls on the basis of written policies and procedures and risk assessments. Off-site reviews do not take place on the premises of subjects of assessment.
Off-site thematic review	means off-site reviews of a number of subjects of assessment, often from the same sector, that focus on one specific or very few aspects of these firms' AML/CFT systems and controls, such as transaction monitoring or the treatment of PEPs. Thematic reviews often serve to help supervisors gain a better understanding of the way specific ML/TF risks are managed by a sector or particular types of credit institutions and financial institutions. Off-site reviews do not take place on the premises of subjects of assessment.
AML/CFT returns	means regular or ad hoc requests to subjects of assessment for quantitative or/and qualitative data and information relating to key ML/TF risk indicators. AML/CFT returns are different from off-site inspections in that they involve a self-assessment by the subject of assessment, are frequently automated and often not comprehensive. Their aim is often to help supervisors gain a better understanding of the ML/TF risks to which their sector is exposed, rather than to assess the adequacy of a firm's AML/CFT systems and controls.
Supervisory action	means action supervisors take to address shortcomings or breaches of credit institutions and financial institutions' AML/CFT obligations. Supervisory action can range from a letter setting out recommendations to the imposition of pecuniary sanctions or the withdrawal of permissions.
ML/TF Risk	means the likelihood and impact of money laundering or terrorist financing taking place.

	Inherent risk refers to the level of ML/TF risk present in a subject of assessment or a sector before mitigating measures are applied and a financial institution's or a sector's **risk profile** refers to the overall characteristics of the ML/TF risk associated with the subject of assessment or sector/subsector, including the type and level of risk.
Emerging risk	refers to a risk that has never been identified before or an existing risk that has significantly increased. Some of the characteristics of emerging risks may include, but are not limited to, the uncertainty as to their actual significance; difficulties to quantify such risks due to lack of data; they may be outside of financial institutions' or CAs' control.
FinTech	means technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services. Some examples of services provided via FinTech solutions: - services enabling cash to be placed on a payment account; - services enabling cash withdrawals from a payment account; - execution of payment transactions; - payment initiation services; - account information services; - e-money services.
BigTech	refers to large technology companies with extensive customer networks; and includes firms with core businesses in social media, internet search, software, online retail and telecoms. Some examples: Google; Apple; Facebook; Amazon; Alibaba (Ant Group); Baidu (Du Xiaoman); Microsoft; Samsung; JD.com; NTT Docomo; Tencent; Rakuten; Mercado Libre.
RegTech	means any range of applications of technology-enabled innovation for regulatory, compliance and reporting requirements implemented by a regulated institution (with or without the assistance of ICT third-party providers). Some examples of AML/CFT activities where RegTech solutions can be used: - CDD ; - customer risk assessment; ongoing monitoring of the business relationship; - transaction monitoring.

Annex 2: Proposals

In addition to the existing EBA's guidelines, the EBA addresses the following proposals to competent authorities, and to European co-legislators.

Cross-sectoral money laundering and terrorist financing risk

Proposals to Competent Authorities

ML/TF risk	Recommendation
Efforts to tackle human trafficking through financial inclusion are disjointed and often inadequate	The EBA advises CAs to understand their sector's exposure to the risk that institutions may be handling the proceeds from human trafficking and take steps commensurate with that risk to mitigate it.
PEPs identification measures remain an important component of the fight against corruption	The EBA advises CAs to understand the risk that institutions in their sector launder the proceeds from corruption or act corruptly themselves.
Competent authorities need to reach out to prudential supervisors in charge of ESG and environmental agencies to strengthen the fight against laundering of proceeds of environmental crime	The EBA advises CAs to understand the risk that institutions in their sector might be laundering the proceeds from environmental crime.
AML/CFT Authorities have a limited awareness of risks associated with laundering the proceeds from cybercrime	The EBA advises CAs to understand their sector's exposure to the risk that they may be used to launder the proceeds from cybercrime.
AML/CFT supervisors and tax authorities need to cooperate more in the fight against tax crimes	The EBA advises CAs to understand the risk that institutions in their sector might be facilitating or laundering the proceeds from tax crimes.
Large cross-border cash transactions pose significant ML/TF risks	The EBA advises CAs to understand the risk of their sector being used for cash-based money laundering.

Proposals to EU co-legislators

ML/TF risk	Recommendation
BigTech can provide financial services but are not always subject to AML/CFT rules or supervision	The EBA advises EU co-legislators to consider including financial services provided by mixed activity groups as obliged entities under the AML/CFT framework.
Virtual IBANs can be abused for ML/TF purposes	If necessary, after the EBA' assessment of risks associated with the misuse of virtual IBANs, the EBA advises the European Commission and EU co-legislators to clarify supervisory expectations and competencies.
Future challenges with Instant payments for implementation of AML	The EBA advises the European Commission and EU co-legislators to require payment service providers providing IPs to identify situations where IPs are not permissible on AML/CFT grounds and to refrain from providing IP services in those cases.

Recommendations to the European Commission

ML/TF risk	Recommendation
Need for further convergence for the supervision of crowdfunding platforms under the AML/CFT framework	The European Commission should assess, as set out in recommendation 6 of the Joint ESAs' response to the European Commission's call for advice on Digital finance, whether to subject crowdfunding platforms licensed under Regulation 2020/1503 to EU AML/CFT legislation, in line with the requirement under Article 45(p) of Regulation 2020/1503.

Money laundering and terrorist financing risks specific to each sector

Recommendations to Competent Authorities

Financial sector	Recommendation
Credit institutions	The EBA advises CAs to test the effectiveness of key AML/CFT controls in banks, including transaction monitoring systems and credit institutions' approaches to identifying and reporting suspicious transactions during inspections and if appropriate, as part of a thematic review. CAs should choose meaningful samples and use these to test system performance.
Payment institutions	The EBA advises CAs to assess how 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. The EBA's Risk Factors Guidelines contains further details. The EBA advises CAs to review their approach to the AML/CFT supervision of payment institutions to ensure that it is sufficiently risk-based and intrusive, in line with provisions in the Risk-based AML/CFT Supervision Guidelines. CAs should focus more on the supervision of agent networks and cooperate more with their counterparts in case of cross-border agent networks.
E-money institutions	The EBA advises CAs to base the frequency and intensity of on-site and off-site supervision on the ML/TF risk profile of individual e-money institutions, and on the ML/TF risks in that sector. The EBA advises CAs to assess how 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. The EBA's Risk Factors Guidelines contains further details.
Bureaux de change	The EBA advises CAs to ensure a sufficiently broad view of AML/CFT systems and controls, especially where bureaux de change offer other financial services such as gold and precious stones trading.

Investment firms	The EBA advises CAs to assess how 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. The EBA's Risk Factors Guidelines contains further details.
Collective investment undertakings	The EBA advises CAs 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.
Fund managers	The EBA advises CAs to consider how best to address the identified weaknesses in controls, such as oversight of AML/CFT framework put in place by fund managers as part of their supervisory approach.
Credit providers	The EBA advises CAs to continue to identify the main risks in each subsector of credit providers and focus their supervisory activities on the areas which represent the highest ML/TF risk in this sector, such as non-performing loans management.
Life insurance undertakings	The EBA advises CAs to consider how best to address the identified weaknesses in controls, such as customer identification and verification, in relation to beneficial owners and PEPs, put in place by life insurance undertakings as part of their supervisory approach.
Crypto-assets service providers	The EBA advises CAs to ensure that their staff receive the adequate and up-to-date training to have the technical skills and expertise necessary for the execution of their functions. The EBA advises CAs to focus their risk assessment on areas identified in the forthcoming amendments to the EBA's Risk Factors Guidelines and the amendments to the Guidelines to prevent the abuse of fund transfers for ML/TF purposes.

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