



JOINT COMMITTEE OF THE EUROPEAN  
SUPERVISORY AUTHORITIES

JC2019 59

---

04 October 2019

---

# Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector

---

## 1. EXECUTIVE SUMMARY

1. In this Joint Opinion, the European Supervisory Authorities (ESAs) identify and analyse, pursuant to Article 6(5) of Directive (EU) 2015/849 (the Anti-Money Laundering Directive — AMLD4), current and emerging money laundering and terrorist financing (ML/TF) risks to which the EU's financial sector is exposed. The ESAs draw on information provided by competent authorities (CAs) and on information obtained in the context of the ESAs' work throughout the year, including a workshop on risks associated with money remitters and e-money issuers organised by them.
2. The ESAs have grouped the risks that were identified throughout this process into two broad categories: cross-sectoral risks and sector-specific risks.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

3. In the cross-sectoral ML/TF risks section of this Joint Opinion, the ESAs have set out current and emerging risks identified by CAs that cut across all sectors and provide a contextual background to these risks. At the time of writing this Joint Opinion, the ESAs had identified that the main cross-cutting risks arise from the withdrawal of the United Kingdom (UK) from the EU; new technologies; virtual currencies; legislative divergence and divergent supervisory practices; weaknesses in internal controls; terrorist financing; and de-risking.
4. One key challenge is the uncertainty generated by the withdrawal of the UK from the EU and associated concerns regarding CAs' ability to adequately supervise the changing population of firms relocating to their Member States from the UK following the withdrawal of the UK from the EU.
5. The ESAs have also found that CAs view the management of risks associated with new technologies, in both FinTech<sup>1</sup> and RegTech<sup>2</sup>, as one of the key challenges prevalent in most sectors. The rapid spread of virtual currencies and recent developments in this area introduced by the Financial Action Task Force (FATF) are also highlighted as growing concerns. Many of these concerns have already been raised by the ESAs via various opinions related to virtual currencies<sup>3</sup> and a report on crypto-assets<sup>4</sup>. To address these risks and concerns, the CAs may need to develop a better understanding of these products and services and their control frameworks, which may be different from the traditional controls that the CAs are familiar with. This may require some degree of engagement between the CAs and the private sector.

---

<sup>1</sup> FinTech, as defined by the Financial Stability Board, 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'.

<sup>2</sup> RegTech, as defined by the Institute of International Finance, means 'the use of new technologies to solve regulatory and compliance requirements more effectively and efficiently'.

<sup>3</sup> EBA Opinion on 'virtual currencies', EBA/Op/2014/08, published on 4 July 2014, available at: <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> and EBA Opinion on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849, published on 11 August 2016, available at: <https://eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD>

<sup>4</sup> EBA report with advice for the European Commission on crypto assets, published on 09 January 2019; available at: <https://eba.europa.eu/-/eba-reports-on-crypto-assets>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

6. This Joint Opinion also highlights concerns about divergent national legal frameworks, which are a direct consequence of the minimum harmonisation framework on which the relevant EU legislation is based, especially in the area of the prevention of the use of the financial system for the purposes of ML/TF. In addition to ML/TF risks arising from divergent transpositions of the AMLD, the ESAs have identified other areas of legislation that may have an impact on ML/TF risks, notably in relation to authorisations, qualifying holdings and assessment of the fitness and propriety of key function holders and members of the management board. These differences have implications for how the anti-money laundering and countering the financing of terrorism (AML/CFT) guidelines and standards developed by the ESAs, which aim to foster convergence across the EU, are implemented in the Member States.
7. In addition to the nature, size and risk rating of the sector, this Joint Opinion emphasises that divergences in the regulatory framework are also contributing to diverging supervisory practices. This Joint Opinion notes significant differences between CAs' supervisory engagements within the same sectors. While such differences may result from a risk-based approach, questions can be raised about some CAs' understanding of relevant ML/TF risks, considering that no assessment of controls has been carried out in some sectors by a large proportion of CAs. Significant differences in resources allocated by Member States to AML/CFT supervision across the single market is also considered a contributing factor to divergent supervisory practices.
8. Furthermore, this Joint Opinion notes that terrorist financing risks continue to be a concern because of ongoing weaknesses in transaction monitoring and limited information flows between law enforcement, firms and CAs.
9. As in the Joint Opinion published in 2017, the CAs remain concerned about firms' implementation of internal controls and their management of emerging risks, particularly the implementation of customer due diligence (CDD) measures. Owing to the interconnected nature of the EU's financial market, such weaknesses can expose the entire EU financial market to a greater risk of ML/TF. In addition, firms' failure to manage ML/TF risks properly, and instead refusing or discontinuing a business relationship with a customer or groups of customers, may



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

lead to de-risking and result in these customers using more informal or unregulated channels for their financial needs. However, from the responses received, the ESAs observed that CAs have developed a better understanding of the quality of controls applied by firms in each sector than they had in 2017. This change may be attributed to increased supervisory activity in certain sectors and the implementation of the ESAs' risk-based supervision guidelines<sup>5</sup>.

10. To mitigate the cross-cutting ML/TF risks identified in this Joint Opinion, the ESAs have proposed a number of potential actions for the CAs. These include:

- (i) ensuring that they are equipped to deal with risks associated with the arrival of new firms and activities into the EU-27 as a result of the withdrawal of the UK from the EU;
- (ii) acknowledging and adapting to the implications of FinTechs and RegTechs;
- (iii) monitoring developments in relation to virtual currencies and assessing if any changes to the national legal and regulatory AML/CFT frameworks are required;
- (iv) setting clear expectations as regards internal controls that safeguard firms from ML/TF risks;
- (v) supporting the exchange of information and cooperation between law enforcement, firms and CAs;
- (vi) guarding against de-risking.

11. In the sector-specific section of this Joint Opinion, the ESAs examined CAs' responses relating to ML/TF risks prevalent in each sector and their assessment of controls put in place by firms to mitigate these risks. Each sector is summarised under the following five subheadings:

- (i) Inherent risk in the sector, where the ESAs have summarised the CAs' assessment of the level of inherent risk associated with each sector. The responses show that, overall, credit

---

<sup>5</sup> Joint Guidelines 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 (ESAs 2016 72) published on 16 November 2016, available at: <https://eba.europa.eu/documents/10180/1663861/Joint+Guidelines+on+Risk-Based+Supervision+%28ESAs+2016+72%29.pdf/7159758d-8337-499e-8b12-e34911f9b4b6>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

institutions, payments institutions, bureaux de change and e-money institutions are considered the most vulnerable to ML/TF.

- (ii) Quality of controls and common breaches in the sector, where the ESAs have outlined their analysis of the CAs' assessment of controls put in place by firms in each sector, which highlights varying levels of deficiencies in all sectors. Overall, it appears that CAs are particularly concerned about the quality of controls relating to the identification and verification of customers, the assessment of risks associated with firms' business and customers, and ongoing monitoring of business relationships, including transaction monitoring. This Joint Opinion recognises that, in some instances, these weaknesses are not mutually exclusive. The ESAs find it particularly alarming that a large proportion of CAs have not carried out an assessment of controls in certain sectors. In addition, this Joint Opinion outlines a summary of the type and seriousness of breaches identified by CAs in each sector. This review highlights that, in the majority of cases, the areas associated with poor-quality controls also result in higher numbers of breaches.
- (iii) Overall risk profile of the sector, where the ESAs have summarised the CAs' assessment of ML/TF risks present in each sector, after consideration is given to the inherent risk and quality of controls. It is evident that, in the majority of cases, the level of overall risk is aligned with the inherent risk ratings, leading to the conclusion that the controls framework may not be sufficiently robust to reduce the overall risk in certain sectors.
- (iv) Emerging risks in the sector, where the ESAs have set out their analysis of the CAs' responses relating to emerging risks in each sector, which shows that the majority of CAs consider new technologies and virtual currencies to present challenges in the future.
- (v) Recommendations for the CAs, where the ESAs have proposed a number of actions for the CAs that may reduce the sector's exposure to ML/TF risks and improve the quality of controls. For example, the ESAs have recommended that those CAs that have not carried out an assessment of controls in certain sectors assess whether or not they hold sufficient information about these sectors to allow them to develop a sufficient understanding of inherent and overall risks in the sector and, as a result, to review their supervisory approach if deemed necessary.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

12. In addition, each subsection includes an assessment of ML/TF risks arising from the sector's exposure to cross-border activities and transactions. Overall, the sectors that are most vulnerable to these risks are credit institutions, e-money institutions, payment institutions, investment firms and investment funds.
13. To complement this Joint Opinion, the ESAs have also developed an interactive tool that gives CAs and firms a quick snapshot of all of the ML/TF risks covered in this Joint Opinion. The interactive tool is available on the EBA's website [http://tools.eba.europa.eu/joint-opinion/JO\\_ML\\_TF\\_2019.html](http://tools.eba.europa.eu/joint-opinion/JO_ML_TF_2019.html); it is based entirely on the information contained in the Joint Opinion and therefore should be used in conjunction with the Joint Opinion.

## 2. BACKGROUND AND LEGAL BASIS

14. Article 6(5) of Directive (EU) 2015/849 (AMLD4) requires the ESAs to issue a Joint Opinion on the ML/TF risks affecting the EU's financial sector. This Joint Opinion serves to inform the European Commission's supranational risk assessment (SNRA) and the ESAs' work on fostering supervisory convergence and a level playing field in the area of AML/CFT. It also serves to inform Member States' CAs in their application of the risk-based approach to AML/CFT supervision. AMLD4 requires the ESAs to publish the Joint Opinion every 2 years and the previous Joint Opinion was published in February 2017.
15. Whereas the requirement to publish this Joint Opinion is set out in AMLD4, the underlying information relates to a period when firms' and CAs' AML/CFT obligations were set out in Directive 2005/60/EC (AMLD3) as transposed into national law by Member States. In accordance with AMLD3, the application of the risk-based approach was suggested, but it was not a mandatory requirement. AMLD3 was later repealed and replaced by AMLD4, which needed to be transposed into Member States' national legislation by 26 June 2017. AMLD4 aims to bring the EU legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted by the FATF, an international AML/CFT standard-setter, in 2012. Like the FATF's standards, AMLD4 puts the risk-based approach at the centre of the EU's AML/CFT regime. It recognises that risks can vary and that



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Member States, CAs and firms must take steps to identify and assess those risks to decide how best to manage them. AMLD4 has been further amended by Directive (EU) 2018/843 (AMLD5), published on 19 June 2018, which Member States are required to transpose into their national legislation by 10 January 2020.

16. Firms carrying out person-to-person transfers also have to comply with Regulation (EU) 2015/847, which requires payment service providers to obtain certain information when processing a transfer.

### 3. METHODOLOGY

17. In drafting this Joint Opinion, the ESAs took into account the views expressed by CAs through a questionnaire related to ML/TF risks and supervisory activities carried out in 2016 and 2017.
18. In total, there are 58 CAs responsible for the supervision of firms' compliance with their AML/CFT obligations in the EU Member States and European Economic Area (EEA) countries. The supervisory framework varies across these countries. In some, the supervision of AML/CFT is divided between a number of different CAs, whereas in others this is the responsibility of one CA. In addition, in some jurisdictions, these CAs are consolidated with authorities responsible for prudential supervision of firms or with Financial Intelligence Units (FIUs). When a CA is also the FIU, information gathered for the purposes of this Joint Opinion relates only to that CA's supervisory obligations.
19. Furthermore, the ESAs organised a number of thematic workshops<sup>6</sup> that brought together CAs, private-sector representatives and representatives of law enforcement to inform their assessment of the ML/TF risks associated with specific sectors. Subject-specific expert reports were also considered as needed and relevant to support the analysis of the information received from CAs.

---

<sup>6</sup> The ESAs organised a workshop at the EBA's premises in London related to money remitters in February 2018 and another workshop related to e-money issues in September 2018.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

20. The methodology used by the ESAs to obtain information from CAs for this Joint Opinion has evolved since the Joint Opinion 2017 was published and hence direct comparisons are not possible in all cases. Although the new methodology requires more detailed information from CAs and was developed with a view to improving the comparison of data and helping to track the development of risks over time, this has proven to be a challenging task for this Joint Opinion. Most of the challenges related to the comparison of data stem from the fact that CAs have different organisational structures and have adopted different supervisory approaches and practices. These differences also apply to how CAs record their supervisory data and carry out their risk assessments. While the ESAs have worked to harmonise the collection and provision of data where possible, data obtained for the purposes of this Joint Opinion may not always be comparable, as the data provided may be based on CAs' perception of risks. In that case, the ESAs' conclusions may be based on qualitative assessments, rather than quantitative data from which trends can be ascertained. Therefore, any data contained in this Joint Opinion have been, and have to be, interpreted in this context.
21. In addition to this Joint Opinion, the ESAs have developed an interactive tool that gives firms and CAs a quick snapshot of the ML/TF risks covered in this Joint Opinion. The interactive tool is available on the EBA's website [http://tools.eba.europa.eu/joint-opinion/JO\\_ML\\_TF\\_2019.html](http://tools.eba.europa.eu/joint-opinion/JO_ML_TF_2019.html). The tool was developed for data visualisation purposes only and is based entirely on the information contained in the Joint Opinion. It does not introduce any additional information.

#### **4. CROSS-SECTORAL MONEY LAUNDERING AND TERRORIST FINANCING RISKS**

22. The protection of the EU's financial integrity depends on, among other factors, firms' ability to prevent and detect ML/TF and the ability of CAs to ensure that firms under their supervision put in place and maintain effective AML/CFT policies and procedures. These policies and procedures include systems and controls to identify, assess and manage ML/TF risks. In addition to the internal control mechanisms that firms are required to put in place, firms often face significant political, technological and business challenges. Therefore, this Joint Opinion provides a



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

contextual background to the risk assessment exercise, taking into account cross-border and emerging ML/TF risks, as well as a number of specific threats that shape the current risk landscape within the EU. At the time of writing this Joint Opinion, the following cross-cutting risks were identified. Some of these risks are the same as, or similar to, the risks identified in the Joint Opinion 2017, such as risks associated with firms' internal controls and terrorist financing; others are emerging risks, including ML/TF risks and challenges associated with the withdrawal of the UK from the EU and the increasing use of new technologies through which financial services are provided.

#### **4.1 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ARISING FROM THE WITHDRAWAL OF THE UK FROM THE EU**

23. On 29 March 2017, the UK notified the European Council of its intention to withdraw from the EU. In the absence of a ratified withdrawal agreement between the EU and the UK, the withdrawal of the UK from the EU will take place on 31 October 2019, unless there is an agreed extension. After the withdrawal of the UK from the EU, the UK will become a 'third country' and will be subject to the same arrangements as other third countries. However, in the case of a withdrawal of the UK from the EU with an agreement, alternative arrangements may be put in place.

24. A withdrawal of the UK from the EU will affect the ML/TF risk to which the EU's financial market is exposed, although the extent of that risk has yet to be determined. The circumstances of the withdrawal of the UK from the EU were, at the time of writing this Joint Opinion, still unclear. The ML/TF risks associated with the withdrawal of the UK from the EU arise from the following:

- (i) CAs' resources: firms hitherto authorised in the UK and providing services to the rest of the EU might look to obtain authorisation and establish themselves in another Member State after the withdrawal of the UK from the EU. This could put a strain on CAs from that Member State, which will have to make sufficient resources available to assess the ML/TF risks associated with the business models and ownership and control structures of a potentially large number of applicant firms. After granting authorisation, these CAs will need to be prepared to supervise those new firms for



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

compliance with their Member State's AML/CFT obligations, among other obligations. There is also a risk that some CAs may not be adequately equipped and staffed to effectively oversee significant numbers of new firms and that the robustness of those Member State's AML/CFT supervision might suffer as a result.

- (ii) CAs' oversight: there is a risk that some of the UK firms that are looking to relocate would establish themselves in another Member State's territory in name only, as 'shell' companies, which would make adequate AML/CFT supervision by the Member State's CA more difficult.
- (iii) Firms' resources: the following firms will be affected by a UK withdrawal from the EU without an agreement:
  - firms authorised in the UK that want to obtain authorisation, establish a branch or provide services in one or more Member States;
  - firms authorised in an EU Member State that want to obtain authorisation in the UK; and
  - firms authorised in an EU Member State that want to maintain business relationships with UK customers.

If, owing to uncertainty over the UK's withdrawal from the EU, a firm's home Member State in the EU will change, it will have to amend and update its AML/CFT policies and procedures to comply with its new home Member State's AML/CFT requirements. Because the AMLD sets only minimum AML/CFT requirements, and more stringent requirements can be applied by each Member State when transposing the AMLD into national legislation, firms' compliance with the existing AML/CFT requirements may not always be sufficient to meet the new home Member State's AML/CFT requirements.

Firms will also have to update their AML/CFT policies and procedures to account for the UK becoming a third country for AMLD purposes. Such changes will be required particularly in relation to correspondent banking relationships, transfers of funds, third-party reliance arrangements and customer risk assessments. Firms should assess



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

the extent of these changes, which could affect their business prior to the withdrawal of the UK from the EU, to eliminate their exposure to increased ML/TF vulnerabilities. Cooperation and information exchange arrangements between the EU/EEA CAs and the UK CAs: in the case of a withdrawal of the UK from the EU without a ratified withdrawal agreement, and in the absence of adequate cooperation arrangements concluded between the EU/EEA CAs and the UK CAs in compliance with Article 57(5) of the AMLD, CAs will no longer be able to exchange relevant information to ensure the effective AML/CFT supervision of firms that operate on a cross-border basis. In the case of a withdrawal of the UK from the EU with an agreement, the exchange of such information will depend on the terms agreed. The EBA agreed, in March 2019, a template for a memorandum of understanding (MoU) outlining provisions of supervisory cooperation and information exchange between the EU supervisory authorities and the UK Prudential Regulatory Authority and the Financial Conduct Authority. The template serves as the basis for bilateral MoUs that are being negotiated and signed by the relevant EU CAs and the UK authorities. This MoU contains some provisions that aim to facilitate the exchange and protection of information for AML/CFT purposes, if permitted by law.

25. The EU institutions, including the ESAs, have been working to minimise the adverse impact that the withdrawal of the UK from the EU may have on the effective functioning of the EU's financial system. For example, the EBA has published two Opinions on preparations for the withdrawal of the UK from the EU<sup>7</sup>, which aim to foster a consistent approach to authorising UK firms across Member States and to put in place arrangements that will ensure the continuation of the cooperation and information exchange between AML/CFT supervisors in the EU and the UK.

---

<sup>7</sup> Opinion of the European Banking Authority on issues related to the departure of the United Kingdom from the European Union, EBA/Op/2017/12, published on 12 October 2017, available at: <https://eba.europa.eu/documents/10180/1756362/EBA+Opinion+on+Brexit+Issues+%28EBA-Op-2017-12%29.pdf> and Opinion of the European Banking Authority on preparations for the withdrawal of the United Kingdom from the European Union, EBA/Op/2018/05, published on 25 June 2018, available at: <https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on+Brexit+preparations+%28EBA-Op-2018-05%29.pdf>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## 4.2 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ARISING FROM NEW TECHNOLOGIES

26. In recent years, ongoing technological developments have opened up new opportunities for FinTech and RegTech providers. However, as described in the ESAs' Opinion on the use of innovative solutions<sup>8</sup>, published in January 2018, these developments may also give rise to additional ML/TF risks.

27. This Joint Opinion highlights that most CAs consider that FinTech and RegTech present ML/TF risks and vulnerabilities, both currently and in the future, to which firms in almost all sectors are exposed to. Nevertheless, CAs appear to have adopted diverging approaches to the assessment of these risks, with some CAs being more advanced in the risk assessment process than others.

28. Those CAs that have carried out a specific assessment on ML/TF risk associated with FinTech identified the following risk-increasing factors:

- the provision of unregulated financial products and services that do not fall within the scope of AML/CFT legislation;
- the quality of information gathered as part of the CDD process, particularly the application of incomplete or ineffective CDD measures;
- a lack of understanding by FinTech providers of their obligations under the AML/CFT legislation and the overall financial regulatory framework;
- different compliance cultures between supervised entities and new FinTech providers;
- an increased use of new technologies to on-board customers remotely, without putting in place proper safeguards, which could increase the firm's exposure to cybercrime, including identity theft;

---

<sup>8</sup> Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, JC/2017/81, published on 23 January 2018, available at: [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf)



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

- an over-reliance on outsourcing arrangements with FinTech firms, without putting in place proper oversight mechanisms.

29. Those CAs that have carried out a formal ML/TF risk assessment on RegTech solutions used by supervised firms highlighted the following risk-increasing factors associated with these solutions:

- firms' over-reliance on information technology solutions, which could lead to a loss of human professional expertise and judgement in monitoring processes;
- a lack of provisions in the current legal framework dealing with RegTech solutions, which means that different standards are applied by different solutions;
- firms' lack of understanding of new technologies that are used in their CDD processes, which may expose firms to ML/TF vulnerabilities;
- when firms are outsourcing all or part of their activities to RegTech providers without proper oversight and governance arrangements in place, it may lead to:
  - difficulties with accessing customer data owing to RegTech providers' potentially short lifespan and with establishing the ownership of that data;
  - questions about the reliability of records held owing to unsound and unsafe record-keeping practices put in place by the RegTech provider;
  - a lack of transparency in the allocation of responsibilities between firms and RegTech providers, particularly when the processes are outsourced to providers that are not obliged entities under the AMLD.

30. Many of these risks are the same as those identified in the ESAs' Opinion on the use of innovative solutions, in which the ESAs reminded firms and CAs of potential vulnerabilities associated with the use of these solutions if they are ill understood or badly applied. Nevertheless, the ESAs also highlighted how the use of these solutions can improve the effectiveness and efficiency of firms' AML/CFT controls.

#### 4.3 RISKS ASSOCIATED WITH VIRTUAL CURRENCIES



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

31. Virtual currencies<sup>9</sup> (VCs) have been the subject of significant media attention over recent years.

However, it is important to remember that VCs are not typically regulated financial products under EU law and therefore customers are exposed to similar risks to those associated with other unregulated products and services. These risks were highlighted by the EBA in an Opinion on 'virtual currencies'<sup>10</sup>, in which the EBA recommended that, in the absence of a sound legal framework, national supervisory authorities should discourage customers and firms from holding VCs and carrying out activities relating to them.

32. To address the increased ML/TF vulnerabilities presented by VCs, the EU legislators included custodian wallet providers<sup>11</sup> 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 in AMLD5, which should be transposed by all Member States by 10 January 2020. This is a welcome change, as it means that these entities must now comply with all relevant AML/CFT requirements. On 9 January 2019, both the EBA<sup>12</sup> and the European Securities and Markets Authority (ESMA)<sup>13</sup> published reports setting out their analyses of the applicability and suitability of EU law to crypto-assets and highlighting the need to remain vigilant about ML/TF risks.

33. Most CAs consider that VCs still give rise to ML/TF risks and they regard VCs as among the most important emerging risks present in almost all sectors for the following reasons:

- a lack of knowledge and understanding by firms and CAs of these products and services, which prevents them from carrying out a proper impact assessment;
- a lack of straightforward regulation governing VCs and associated products and services;
- increased processing of transactions online, with only limited customer identification and verification checks being carried out.

---

<sup>9</sup> 'Virtual currencies' is used here as defined in Article 3(18) of AMLD4.

<sup>10</sup> EBA Opinion on 'virtual currencies', EBA/Op/2014/08, published on 4 July 2014, available at: <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

<sup>11</sup> 'Custodian wallet providers' is used here as defined in Article 3(19) of AMLD4.

<sup>12</sup> Report with advice for the European Commission on crypto-assets, EBA Report, published on 9 January 2019, available at: <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf>

<sup>13</sup> Advice: initial coin offerings and crypto-assets, ESMA50-157-1391, published on 9 January 2019, available at: [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf)



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

34. Moreover, in October 2018, the FATF adopted amendments to its Recommendation (Recommendation 15 and the Glossary) to include a definition on 'virtual assets' (instead of VCs) and 'virtual asset service providers'. As a result, a wider range of products and services now fall within the scope of the FATF standards than those covered by the current EU AML/CFT legal framework (e.g. crypto-to-crypto exchanges).

35. In conclusion, although AMLD5 has expanded the scope of obliged entities, which, when transposed into national law, will address some of the risks associated with VCs, further actions are considered appropriate (see the EBA's Report with advice for the European Commission on crypto-assets<sup>14</sup>).

#### 4.4 RISKS ARISING FROM LEGISLATIVE DIVERGENCE

36. The ESAs consider that the EU's financial sector continues to be exposed to ML/TF risks because Member States have transposed EU law into national legislation in different ways. While differences in national law are expected and justified when the underlying directive is a minimum harmonisation directive, there are also some provisions in EU law that have been interpreted differently by Member States, including provisions on the risk-based approach. The resulting divergence could have a significant impact and could have negative implications for the robustness of the EU's AML/CFT defences, as well as for the integrity and stability of the EU's financial market.

37. The ESAs are particularly concerned about ML/TF risks arising from legislative divergence in the following four areas:

- (i) The AMLD's minimum harmonisation nature and directive-based approach affect the level of convergence that the ESAs' AML/CFT standards and guidelines can achieve. For example, there is some evidence that some firms obtain authorisation in Member States whose AML/CFT regimes they perceive to be more permissive, with a view to providing services in other Member States from this base.

---

<sup>14</sup> Report with advice for the European Commission on crypto-assets, EBA Report, published on 9 January 2019, available at: <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

- (ii) For much of the period covered by this Joint Opinion, the respective responsibilities of home and host AML/CFT supervisors were interpreted differently in Member States. There was a risk, which materialised in a number of cases, that different national interpretations of relevant provisions in Union law could mean that some firms' operations were not supervised, or not monitored effectively, for compliance with their AML/CFT obligations. AMLD4 brings some clarity in this respect.
- (iii) The EU's rules on authorisations, qualifying holdings, and fitness and propriety rely heavily on national transpositions and interpretations of EU law by national prudential supervisors and the European Central Bank (ECB). They leave little room for the development of a consistent EU approach to addressing ML/TF risk effectively in these contexts. For example, the way that EU law has been transposed in some Member States means that some CAs are of the view that they are unable to act on ML/TF concerns unless they can find evidence of criminal convictions. This is of concern because, once a firm is authorised, the passporting rights attached to some forms of licence (e.g. for banking and payment services) enable it to provide its services across the EU unhindered and so ML/TF risks can be spread by the firm across a number of Member States. It is, therefore, important to reconsider the way that the legal provisions governing prudential supervision of firms are drafted by legislators and interpreted by Member States and prudential authorities, to ensure that AML/CFT issues are given the attention they need and that CAs can intervene where necessary. In this context, the ESAs welcome recent legislative developments, including proposed changes to the Capital Requirements Directive V, which bring greater legal clarity in this area.
- (iv) At the same time, cooperation between CAs that are responsible for the AML/CFT supervision of firms that operate on a cross-border basis and cooperation between CAs and prudential supervisors was sometimes hampered by real or perceived legal obstacles related to the exchange of information. In addition, there was no explicit duty to cooperate in this regard. There was a risk that supervisors had only a partial view of the risks associated with certain sectors or firms. The ESAs expect that legal changes introduced by AMLD5 will provide a clear legal basis for supervisory cooperation. This will be



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

complemented by a clear framework for the exchange of information set out in the ESAs' supervisory cooperation guidelines<sup>15</sup> and, to a certain extent, in the multilateral agreement<sup>16</sup> on the practical modalities for exchange of information between the ECB and the CAs.

#### 4.5 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ARISING FROM DIVERGENT SUPERVISORY PRACTICES

38. Since the Joint Opinion 2017, AML/CFT supervision in the EU has been in the spotlight perhaps more than ever before. The FATF and Moneyval, in their mutual evaluations, question the adequacy of some CAs' approaches to AML/CFT supervision. Members of national parliaments, as well as the European Parliament, are also looking into CAs' responses to various allegations of AML/CFT failures and find some of these responses to be lacking. The EBA has concluded its first ever breach of Union law case against an AML/CFT supervisor<sup>17</sup>. In addition, continuing allegations of breaches of applicable AML/CFT rules by a number of large firms have raised the question of whether or not a more robust and consistent approach to monitoring and testing firms' AML/CFT compliance across the EU could have prevented these failures from happening.

39. To develop a better understanding of potential root causes of these issues, the ESAs' survey contained a large section of questions relating to the CAs' approaches to supervision. In light of the events highlighted above, there is a tendency to generalise the AML/CFT supervision across the EU and assume that it is consistent in all Member States. However, the responses to the survey highlight that national approaches continue to differ significantly between CAs in different jurisdictions. Various factors that may contribute to these differences, including the

---

<sup>15</sup> Consultation Paper on draft joint guidelines on the cooperation and information exchange for the purposes of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (JC/CP/2018/59); published on 08 November 2018; published on: <https://eba.europa.eu/-/esas-consult-on-guidelines-on-cooperation-and-information-exchange-for-aml-cft-supervision-purposes>

<sup>16</sup> Pursuant to Article 57a(2) of Directive (EU) 2015/849, the ESAs supported the conclusion of a Multilateral Agreement between the ECB and AML/CFT competent authorities in the EU. A copy of the Multilateral Agreement is available at: <https://eba.europa.eu/documents/10180/2545547/Agreement+between+CAs+and+the+ECB+on+exchange+of+information+on+AML.pdf/e83dd6ee-78f7-46a1-befb-3e91cedeb51d>

<sup>17</sup> EBA issues recommendation to the Maltese Financial Intelligence Analysis Unit in relation to its supervision of Pilatus Bank, 11 July 2018, available at: <https://www.eba.europa.eu/-/eba-issues-recommendation-to-the-maltese-financial-intelligence-analysis-unit-in-relation-to-its-supervision-of-pilatus-bank>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

differences in the national transposition of the AMLD, variations in the size and nature of the supervised sector and the level of exposure to ML/TF risk. Any gaps in the AML/CFT supervisory framework, if exploited, could potentially have significant implications for the robustness of the EU's AML/CFT defences and for the integrity and stability of the financial market.

40. The main differences observed by the ESAs relate to the frequency and intensity of supervisory engagements with firms in different sectors, which are often justified by differing levels of risks in these sectors and the resource constraints at the CA. The review of responses confirms that most CAs focused their attention on sectors they considered to present significant ML/TF risks, while often neglecting sectors perceived to be less risky (see Figures 1 and 2 for more details). This may be in line with the risk-based approach<sup>18</sup>, in which, on the basis of reliable information, the CA has developed a good understanding of the ML/TF risks to which each of their sectors is exposed. However, this appears to have been challenging for some CAs. There is evidence to suggest that, in some cases, CAs have based their assessment of ML/TF risk associated with a particular sector in their jurisdiction solely on one risk factor, or applied the ML/TF risk assessment of another Member State's CA almost unquestioningly to their own sector. There is a risk that, by failing to obtain a holistic view of relevant risk factors prevalent in a particular jurisdiction and failing to tailor the risk assessment to each sector in the context of each Member State, CAs may fail to identify, and act upon, ML/TF risks to which their sector is exposed. The ESAs' guidelines on risk-based AML/CFT supervision, which came into effect in April 2017 and which needed to be implemented by April 2018, will support CAs' risk assessment efforts going forward.

41. Furthermore, the number of specialist AML/CFT staff employed by CAs varies significantly. While differences are expected and acceptable under the risk-based approach, responses to the ESAs' questionnaires and findings from international assessments<sup>19</sup> suggest that the level of resources

---

<sup>18</sup> For more details on the risk-based approach, see the Joint Guidelines 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, ESAs 2016 72, published on 16 November 2016, available at: <https://eba.europa.eu/documents/10180/1663861/Joint+Guidelines+on+Risk-Based+Supervision+%28ESAs+2016+72%29.pdf/7159758d-8337-499e-8b12-e34911f9b4b6>

<sup>19</sup> For more details on mutual evaluations carried out by the FATF and Moneyval, see: [http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate))



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

and AML/CFT supervision is not always commensurate with the level of ML/TF risk and the size of the sector in all Member States.

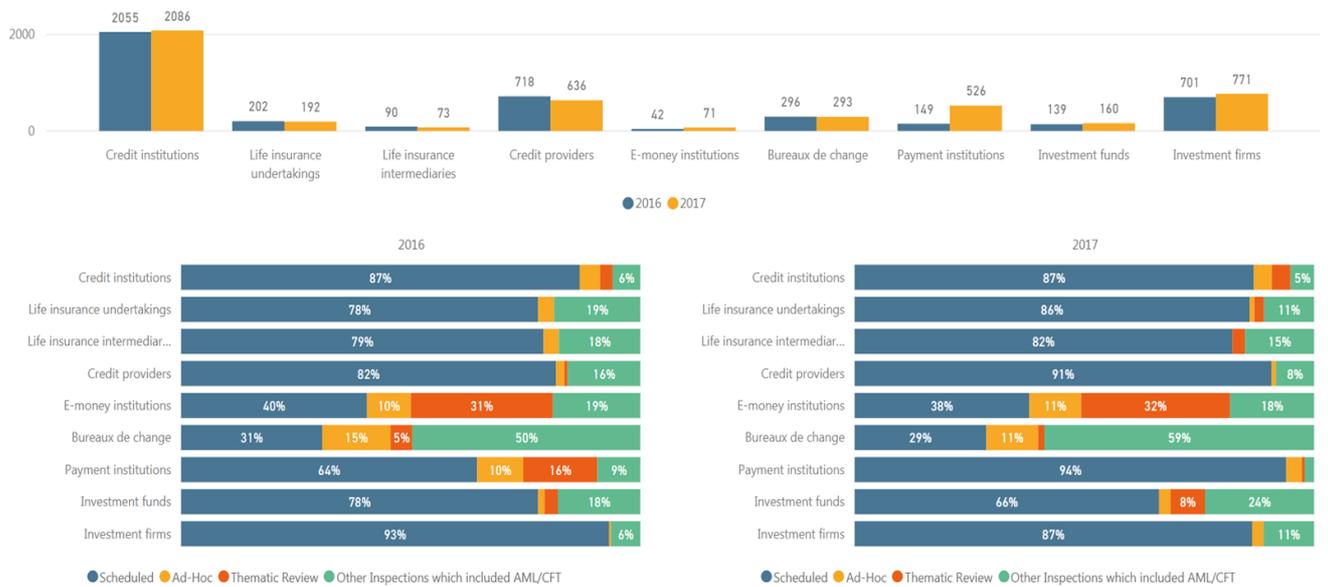


Figure 1: Number of onsite inspections per sector and the type of inspections carried out in each sector — 2016 versus 2017.

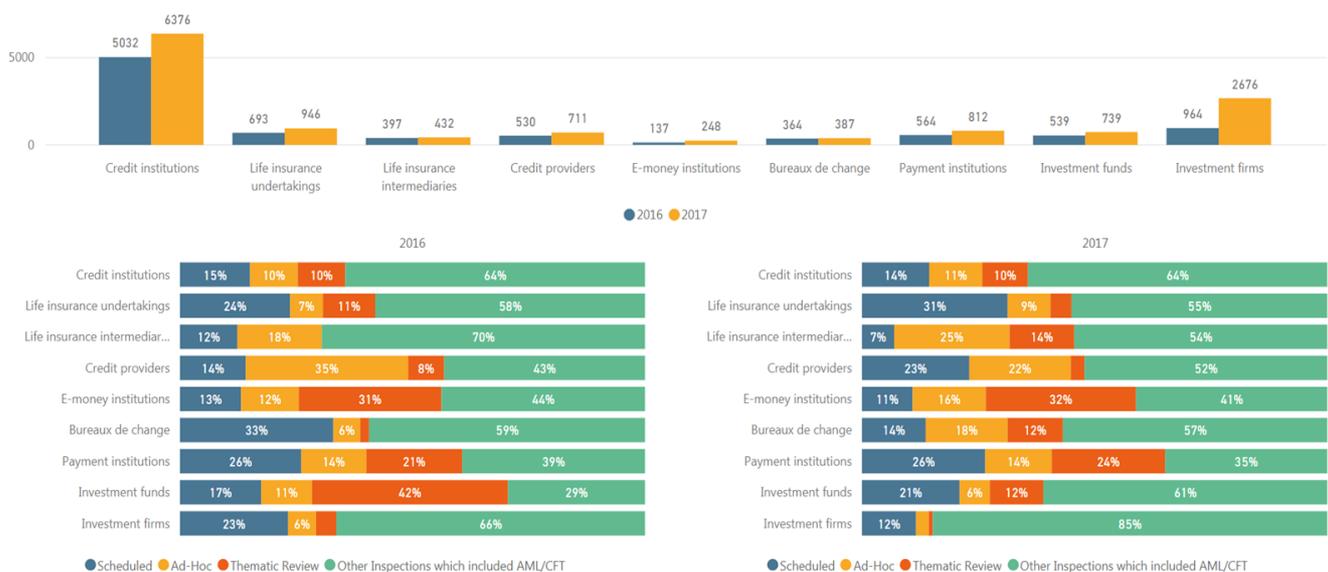


Figure 2: Number of offsite inspections per sector and the type of inspections carried out in each sector — 2016 versus 2017.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

#### 4.6 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ARISING FROM WEAKNESSES IN INTERNAL CONTROLS

42. In line with AMLD4, firms are required to put in place an internal systems and controls framework that is commensurate with the ML/TF risk to which that firm's business is exposed. When the internal controls are inadequate, a firm's business is more vulnerable to ML/TF risks. Therefore, an outcome of supervisory activity is the assessment of firms' quality of controls and potentially the identification of breaches of legislation.

43. In contrast with the Joint Opinion 2017, the majority of CAs responding to this Joint Opinion have rated internal systems and controls put in place by their supervised firms as either good or very good. Most CAs consider policies and procedures implemented by firms to be adequate, particularly in respect of record-keeping, identification and verification of customers, and suspicious transaction reporting (STR). However, data received by the ESAs highlight that the application of these policies and procedures in practice is not consistently effective. In relation to the effectiveness of these policies and procedures, of particular concern to CAs are the quality of business-wide ML/TF risk assessments, the effectiveness of STR and the effectiveness of ongoing policies and procedures, including transaction monitoring. These controls were rated as poor or very poor by a number of CAs (see Figures 3 and 4).

44. Another area of concern for CAs identified in the Joint Opinion 2017 was the adequacy of firms' AML/CFT resources. Since then, this area appears to have improved and data received for this Joint Opinion in respect of 2016 and 2017 show that the majority of CAs did not raise any concerns about firms' AML/CFT resources.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

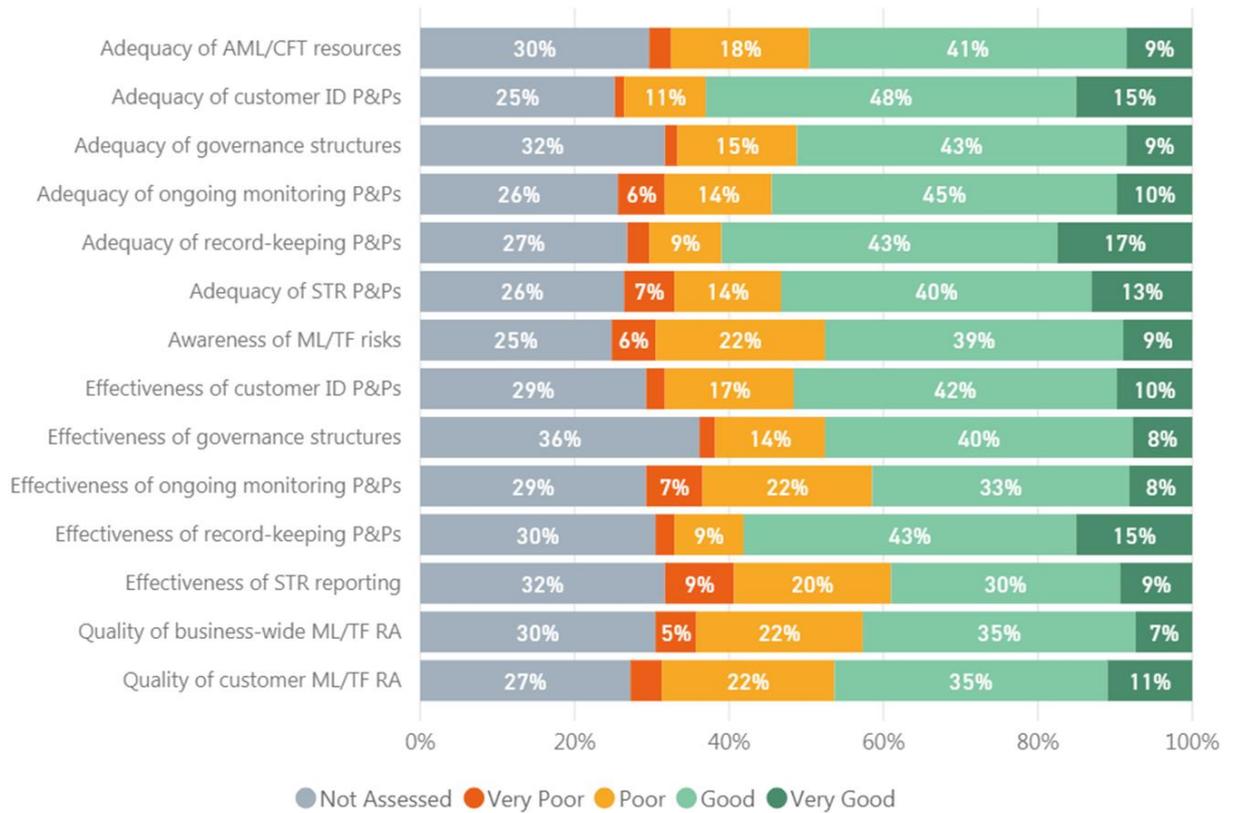


Figure 3: Overall quality of controls in all sectors in 2016. (In this figure, 'RA' means a risk assessment and 'P&Ps' means policies and procedures.)



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

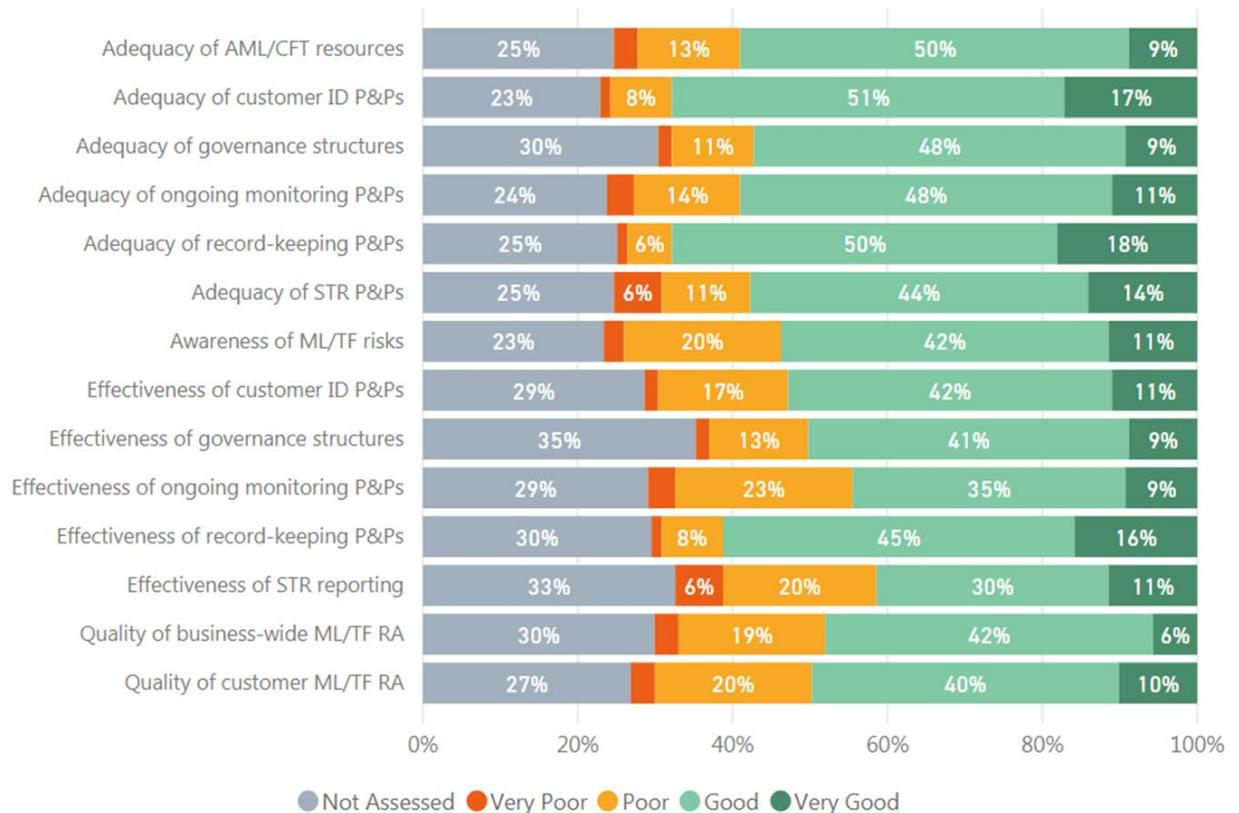


Figure 4: Overall quality of controls in all sectors in 2017. (In this figure, ‘RA’ means risk assessment and ‘P&Ps’ means policies and procedures.)

45. When CAs were asked to identify the most common types of breaches of legislation, these related to inadequate controls as regards the identification and verification of firms’ customers, weaknesses in the internal controls and overall AML/CFT policies and procedures, and customer risk assessments. Statistics for 2017 largely correspond to statistics for 2016 (see Figure 5).

46. In addition, CAs are also concerned about the systems and controls put in place by firms for the identification and verification of beneficial owners, as they consider them inadequate. In line with the ESAs’ Risk Factors Guidelines<sup>20</sup>, if a firm is unable to identify a beneficial owner because

<sup>20</sup> Joint Guidelines by the European Supervisory Authorities under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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 (JC 2017 37), published on 26 June 2017; available at: <https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

the customer has gone to great lengths to disguise it by forming various complex structures, the firm should consider the reasons for such behaviour, as it might be an indicator that the business relationship presents a high ML/TF risk. Some CAs suggest that the lack of publicly available registers containing sufficient data on beneficial ownership is a contributing factor to these shortcomings. However, the ESAs consider that reliance on such registers for the purpose of identifying the beneficial owner is not warranted in all cases. Instead, these registers are useful as an additional source of information when verifying the beneficial owner's identity, but they cannot be the only source of information used for identification, in particular in situations in which the ML/TF risk associated with a business relationship is increased.

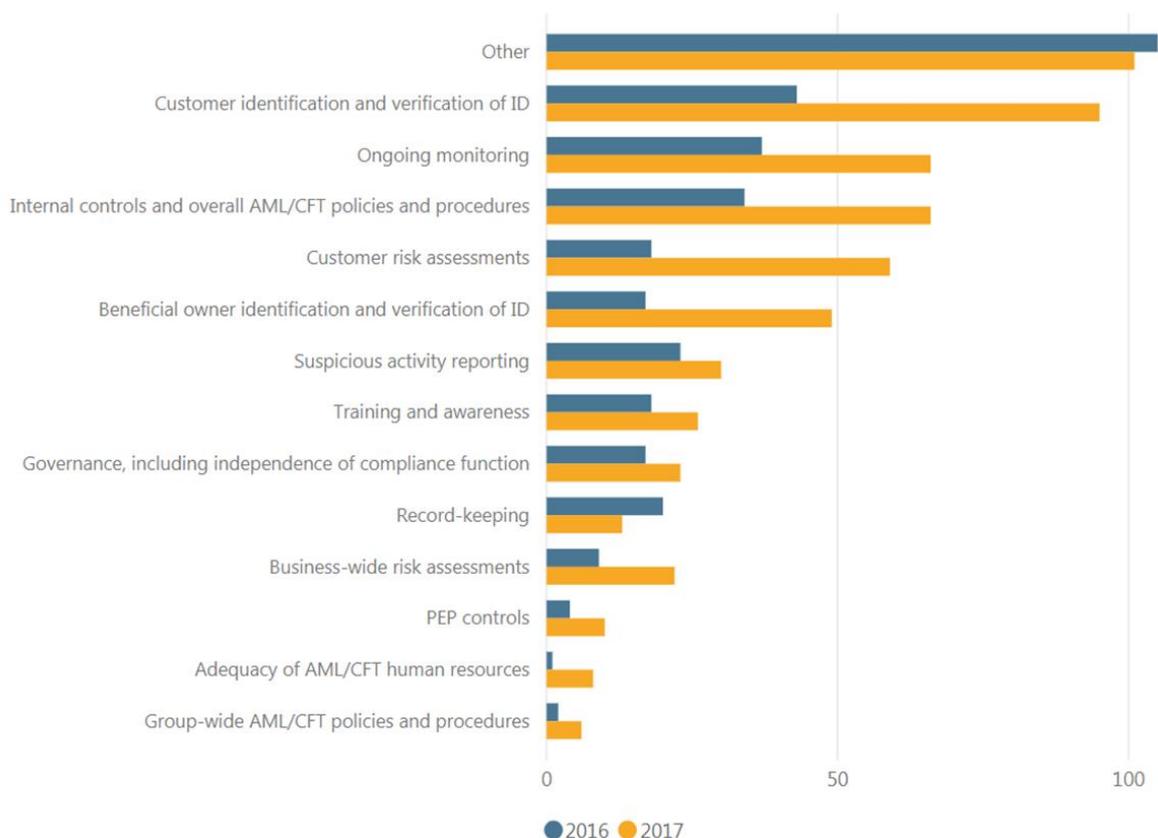


Figure 5: Most common types of breaches identified by CAs in 2016 and 2017 across all sectors. (In this figure, 'PEP' means a politically exposed person.)



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

#### 4.7 TERRORIST FINANCING RISK

47. The ESAs consider that the EU's financial sector continues to be exposed to terrorist financing (TF) risks and find that the observations set out in the Joint Opinion 2017 are still relevant. AML/CFT systems and control weaknesses in firms or sectors that are perceived to be particularly vulnerable to abuse for TF purposes continue to persist. This is of concern because the systems and controls that firms put in place to mitigate TF risks are similar to, and often the same as, the controls put in place for anti-money laundering purposes.

48. Feedback from CAs points to persistent weaknesses in systems and controls related to firms' transaction monitoring. In contrast with money launderers, individuals looking to finance terrorism may not seek to hide their identity and may use legitimate funding sources, often in small amounts. This means that the measures that firms put in place to identify their customers and verify their identities may carry less weight in the context of countering the financing of terrorism (CFT) than effective ongoing monitoring of transactions. What is more, contrary to common perceptions, sanctions screening is not a substitute for effective, risk-based CFT controls. Financial sanctions target individuals or groups that are already known to pose a threat, whereas TF risk often emanates from individuals who are not caught by the sanctions regime. This is why risk-based AML/CFT controls, and transaction monitoring in particular, are key to the effective fight against TF.

49. The fight against TF continues to be hampered by firms not having access to relevant information — often held by law enforcement agencies — that would help them identify TF risks before they crystallise. Likewise, law enforcement agencies' efforts to disrupt terrorist activities and networks can be hampered when they are unable to obtain information about terrorist finance flows that only firms can provide. It is essential, therefore, that law enforcement, CAs and firms work closely together in the fight against TF.

50. Taking this into account, the ESAs welcome the fact that there are now a small number of initiatives at the national and supranational levels that are designed to test how law enforcement agencies can provide firms with more specific and meaningful information on specific persons of interest, allowing firms to focus their transaction monitoring on these



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

persons. These initiatives do not replace, but are run in addition to, firms' standard practices for reporting suspicious transactions. Feedback from firms and law enforcement agencies suggests that some firms may be reluctant to participate in such initiatives because of concerns about potential privacy and data protection implications. Firms are also concerned that, if a firm has identified a specific person of interest to the law enforcement agencies on its database, it may be viewed by CAs as a weakness in the firm's systems and controls framework and result in an administrative sanction.

#### 4.8 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ARISING FROM DE-RISKING

51. The ESAs consider that the EU's financial sector continues to be exposed to ML/TF risks arising from financial exclusion. A lack of access to the financial system can drive financial transactions underground and away from effective AML/CFT oversight and controls. Often, such financial exclusion is the result of de-risking, that is, a decision taken by firms to no longer offer services to some categories of customers associated with higher ML/TF risk. This is particularly concerning in the terrorist financing context, as these higher risk customers, or their customers (where the customer is itself a financial institution), will increasingly resort to informal or unregulated payment channels to meet their financial needs or to service a particular segment of customers. In such circumstances, these persons often resort to using cash, which means that these transactions are no longer traceable, making the detection and reporting of suspicious transactions and, ultimately, the prevention of terrorist attacks more difficult.

52. The ESAs in their guidelines are clear that the application of a risk-based approach does not require firms to refuse, or terminate, business relationships with entire categories of customers that are considered by firms to present higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one category<sup>21</sup>. However, industry feedback and discussions at the EBA's workshop on money remitters suggest that de-risking continues to be

---

<sup>21</sup> Joint Guidelines by the European Supervisory Authorities under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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 (JC 2017 37), published on 26 June 2017; available at: <https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

of concern and that no progress has been made since the last Joint Opinion was published<sup>22</sup>. National governments and CAs therefore need to do more to ensure that legitimate customers are not being denied access to the financial system unnecessarily, as such actions may have an adverse effect, whereby, instead of preventing ML/TF, firms may increase the overall internal market's vulnerability to ML/TF risks.

#### 4.9 CONCLUSIONS AND A PROPOSED WAY FORWARD

53. Most of the information used in this Joint Opinion refers to the assessment of ML/TF risks and supervisory activities carried out by CAs in 2016 and 2017. Like in the last Joint Opinion, it is evident that most challenges related to the AML/CFT framework in the EU stem from the fact that AMLD4 is a minimum harmonisation directive, which means that the ways that Member States transpose it in their national legislation may differ.

54. Some of the underlying factors that gave rise to the ML/TF risks identified in this Joint Opinion have since been addressed by firms and CAs. For example, since the last Joint Opinion was issued, AMLD4 had to be transposed; in addition, the ESAs published a number of draft regulatory technical standards and guidelines, which had not been fully implemented in all Member States at the time when data were gathered for this Joint Opinion. Together, these standards and guidelines create a common understanding, on the part of CAs and firms, of the risk-based approach to AML/CFT and how it should be applied. Therefore, the effective implementation of these standards and guidelines is essential, as a more consistent approach will reduce the EU's vulnerabilities to ML/TF risks.

55. In addition, to address the shortcomings in the AML/CFT supervisory framework, throughout 2018, the European Commission, the European Parliament and the European Council each issued proposals and action plans to improve AML/CFT supervision in the EU going forward<sup>23</sup>.

---

<sup>22</sup> See page 10 of the Joint Opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector, JC/2017/07, published on 20 February 2017, available at: <https://eba.europa.eu/documents/10180/1759750/ESAS+Joint+Opinion+on+the+risks+of+money+lauding+and+terrorist+financing+affecting+the+Union%E2%80%99s+financial+sector+%28JC-2017-07%29.pdf>

<sup>23</sup> For more details, see: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/624424/IPOL\\_IDA\(2018\)624424\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/624424/IPOL_IDA(2018)624424_EN.pdf) and <https://www.consilium.europa.eu/media/37283/st15164-en18.pdf>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Meanwhile, the EBA has launched a programme of implementation reviews in which it is assessing the CAs' approaches to the AML/CFT supervision of credit institutions.

56. Recent events have also highlighted that cooperation between CAs in different Member States is not always effective. For that reason, the ESAs have drafted guidelines on supervisory cooperation, which, when implemented, will raise awareness and improve convergence in the CAs' actions when supervising firms that operate on a cross-border basis. Therefore, the ESAs urge CAs to implement these guidelines as soon as they are issued.

57. To mitigate the ML/TF risks identified in this Joint Opinion, the ESAs consider that CAs should take the following steps:

- (i) To mitigate the ML/TF risks associated with the withdrawal of the UK from the EU, and in particular the strain on CAs' supervisory resources caused by UK-authorized firms looking to establish themselves in Member States after the withdrawal of the UK from the EU, CAs should assess whether or not, and if so how, they can make better use of existing arrangements to ensure cooperation and information exchange between them and the UK authorities, including in the AML/CFT context and the wider, prudential, context to the extent that ML/TF risks are concerned.
- (ii) To mitigate the risks associated with new FinTech firms or to ensure firms using RegTech solutions meet their AML/CFT obligations, CAs should acknowledge the changing AML/CFT landscape, particularly the fact that, increasingly, more customers are on-boarded without face-to-face contact; CAs should familiarise themselves with these technological developments by engaging directly with providers and firms, even when they are not supervised entities.
- (iii) As the use of virtual currencies is continually growing, the need to regulate this sector and associated businesses is continually discussed by the ESAs and the EU legislators. In particular, in April 2019, the European Commission confirmed that it is taking forward analytical work further to the January 2019 advice of the EBA and ESMA, and the ESAs are continuing their work to promote convergence in regulatory and supervisory approaches to virtual currencies. In addition, the FATF has made further amendments to its



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Recommendations to cover virtual assets. Therefore, CAs should closely monitor any developments in this area and assess if any changes to the national legal and regulatory AML/CFT frameworks are required.

- (iv) To mitigate the risks associated with the ineffective implementation of internal controls and the failure to adequately manage emerging risks, which was prevalent across all sectors and in all Member States, CAs should prioritise the setting of clear regulatory expectations in this field, including by referring to the ESAs' risk factors guidelines. This may also include CAs focusing their supervisory activities on internal controls that safeguard firms from the highest ML/TF risks.
- (v) It is evident that, in order to have a robust framework for fighting terrorist financing, firms, law enforcement agencies, FIUs and CAs should work closely together, as each side holds information that may be relevant for the other. Therefore, CAs need to do more to support this exchange of information and provide reassurance to firms that cooperation with law enforcement is both useful and necessary and, in most cases, is possible under the applicable legal framework.
- (vi) Evidence suggests that certain customers and customer groups are still prevented from obtaining financial services owing to risks presented by them, which is known as de-risking. As discussed in this Joint Opinion, such actions by firms may have an adverse effect, whereby these customers resolve to meet their financial needs through less reliable or unregulated means. As a result, these transactions are not monitored and reported to the FIUs. Therefore, CAs should work with firms and affected customers to identify solutions for making sure that AML/CFT measures do not unduly deny legitimate customers access to financial services.

58. As noted in this Joint Opinion, there are certain risks and weaknesses that have remained unchanged since the last Joint Opinion was issued. To address this, the ESAs should:

- (i) assess the effectiveness of the implementation of their standards and guidelines through the implementation reviews led by the EBA, with a view to identifying good practices and highlighting areas that should be improved;



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

- (ii) ensure that adequate equivalence provisions that allow cooperation and information exchange with the UK CAs are swiftly available after the withdrawal of the UK from the EU to ensure continuity of the supervision of firms that are looking to operate in the EU;
- (iii) help CAs to develop their understanding of opportunities and ML/TF risks associated with new technologies and enhance supervisory convergence related to these technologies — this could may be achieved through amendments to the ESAs' Risk Factors Guidelines and through guidelines or best practices for AML/CFT supervisors on approaches to supervising new technologies, as well as through organised training;
- (iv) consider ways in which information exchange between law enforcement agencies, FIUs, CAs and firms could be improved.

59. The European Commission should consider the risks and challenges addressed in this Joint Opinion. When deciding on the future of AML/CFT supervision in Europe, as outlined in the Council's 2018 Action Plan, the European Commission should also give due consideration to risks arising from the minimum harmonisation nature of Europe's AML/CFT framework and the different ways in which Member States have incorporated it into national legislation.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## 5. MONEY LAUNDERING AND TERRORIST FINANCING RISKS SPECIFIC TO EACH SECTOR

60. This section of the Joint Opinion provides a summary of CAs' responses to the ESAs' ML/TF risk questionnaires, in which CAs were asked to provide information about each sector's overall risk profile, inherent risks<sup>24</sup> and vulnerabilities associated with the sector, and their assessment of risk-mitigating measures taken by firms. Responses received from CAs are based on a combination of qualitative and quantitative data<sup>25</sup> gathered either as a result of their supervisory activities or as part of their risk assessment. In some instances, an assessment is based on an informed estimate of ML/TF risks, which predates a formal risk assessment. The relevant period covered 2016 and 2017. Where relevant, information from other sources, such as the ESAs' sector-specific ML/TF risk workshops, is also reflected in this Joint Opinion.

61. In total, there are 58 CAs in the EU Member States and EEA countries responsible for the supervision of firms' compliance with AML/CFT rules; however, not all of them are responsible for all sectors and, in some jurisdictions, there might be two different CAs responsible for the supervision of firms in one sector.

### 5.1 CREDIT INSTITUTIONS

62. In total, 33 CAs, which are responsible for supervising the compliance of credit institutions<sup>26</sup> (CIs) with AML/CFT obligations, responded to the ESAs' questionnaire<sup>27</sup> in respect of data for 2016 and 30 CAs responded in respect of data for 2017.

---

<sup>24</sup> Inherent risk refers to the level of ML/TF risk before mitigation and the overall risk profile refers to the risk that remains after both inherent risks and controls have been considered.

<sup>25</sup> A combination of qualitative and quantitative data would include a risk assessment prepared in line with the ESAs' risk-based supervision guidelines.

<sup>26</sup> 'Credit institutions' is used here as defined in Article 3(1) of AMLD4.

<sup>27</sup> In some Member States, more than one authority is responsible for the AML/CFT supervision of credit institutions.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## I. INHERENT RISK IN THE SECTOR

63. The CI sector is considered inherently risky from an ML/TF risk point of view, as CIs are often the first point of entry into the overall financial system. Overall, the sector is extremely diverse in terms of its nature, scale and complexity and this is also reflected in the CAs' responses to questions related to the inherent ML/TF risk ratings, which range from very significant to less significant (see Figure 6 for more details). While the concentration of CIs that are considered as presenting a very significant ML/TF risk is relatively small in terms of the number of institutions, these CIs represent the largest CIs operating in the EU, which offer a variety of different products and services to diverse groups of customers across different Member States.

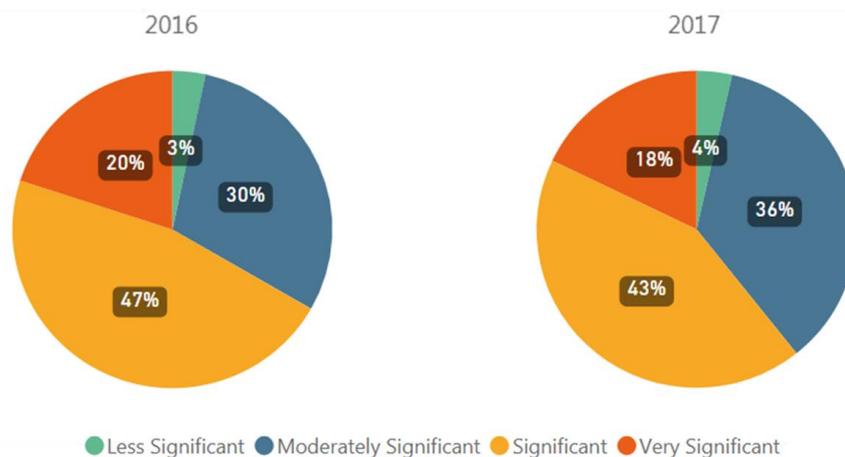


Figure 6: Inherent ML/TF risk profile of the credit institution sector — 2016 versus 2017.

64. The use of cash is still considered by most CAs as one of the contributing factors that exposes the sector to ML/TF vulnerabilities, particularly as the sector is made up of many retail banks. However, the extent to which cash is used varies between Member States.

65. Many CAs are also concerned about the sector's exposure to cross-border transactions and considers them to present significant and moderately significant ML/TF risk (see Figure 7 for more details), particularly in those Member States that are known as international financial centres. Customers that are off-shore companies or individuals from high-risk jurisdictions also contribute to the increased inherent risk in this sector.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

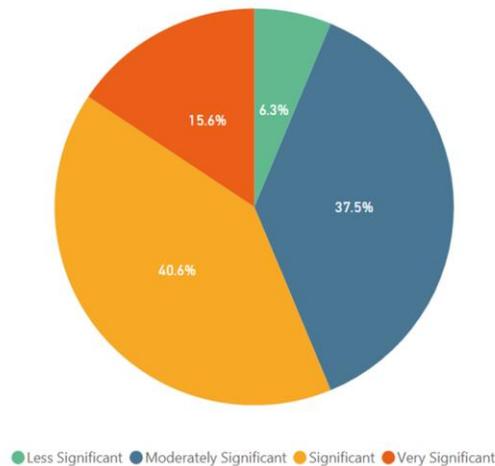


Figure 7: Credit institution's exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

66. Most CAs assessed the controls put in place by CIs as good or very good overall. This was in spite of CAs considering that the effectiveness of AML/CFT policies and procedures, particularly those related to ongoing monitoring of transactions and STRs, is poor or very poor (see Figure 8 for more details).

67. A significant number of CAs pointed to problems associated with risk assessments. They are particularly concerned about the adequacy of both the business-wide risk assessments and CIs' risk assessments associated with individual business relationships. In particular, CAs are not satisfied with CIs' understanding of risks associated with complex off-shore structures and controls put in place by CIs for the identification of beneficial ownership for these structures. In some instances, it transpired that CAs have not assessed this area at all. CIs' controls relating to ongoing monitoring and STRs have also raised concerns for CAs.

68. Overall, CAs appear to be relatively satisfied that the required systems and controls have been put in place by CIs, but they appear to be more concerned about (1) the quality and effectiveness of these controls when applied in practice and (b) the level of CIs' understanding of risks that they are exposed to. This gives rise to significant concerns that some CIs are failing to effectively



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

detect and deter ML/TF and that more work in this area may be required from CAs to address these shortcomings.

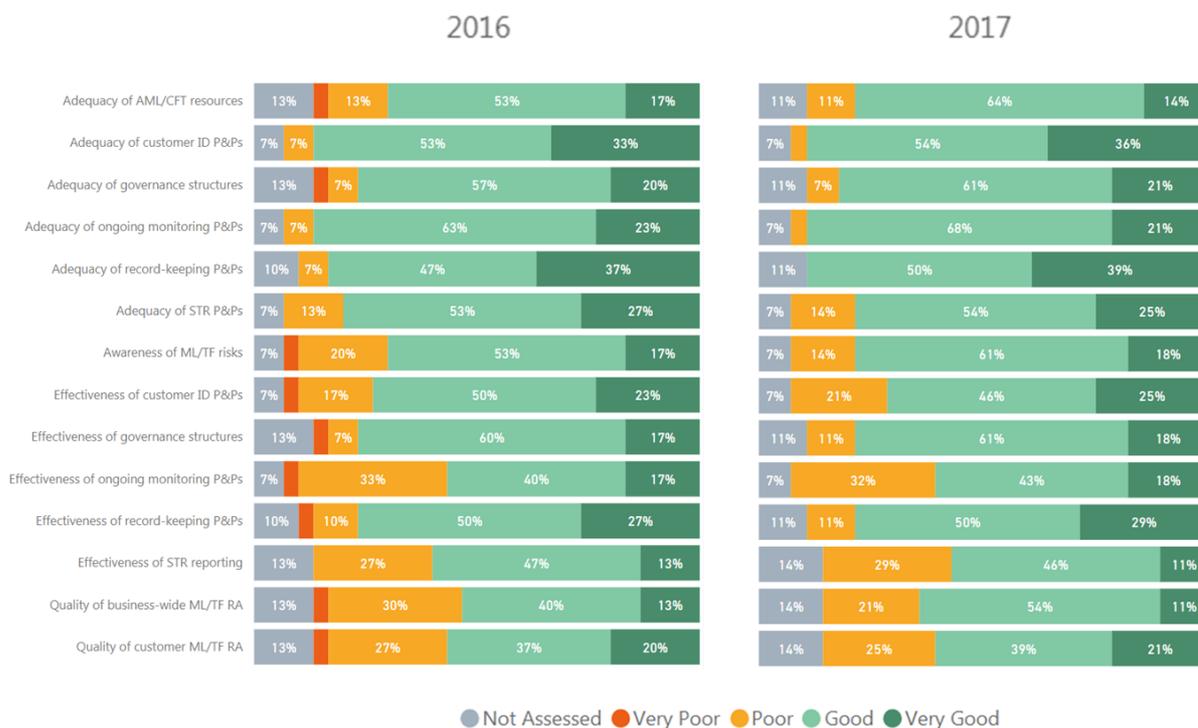


Figure 8: Quality of controls in the credit institution sector — 2016 versus 2017.

69. It is evident from Figures 1 and 2 that the CI sector has the highest supervisory activity in comparison with other sectors. This is in line with the risk-based approach as set out in the ESAs' risk-based supervision guidelines<sup>28</sup>, which require that the intensity of supervisory activities and the level of supervisory resources are commensurate with the ML/TF risk presented by a firm. As a result, the CAs have identified a large number of breaches, which range from minor to egregious in their severity (see Figure 10 for more details). From the responses received, it appears that the main breaches in this sector relate to the identification and verification of customers and beneficial owners, customer risk assessments and STRs (see Figure 9 for more details).

<sup>28</sup> Joint Guidelines 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, ESAs 2016 72, published on 16 November 2016, available at: <https://eba.europa.eu/documents/10180/1663861/Joint+Guidelines+on+Risk-Based+Supervision+%28ESAs+2016+72%29.pdf/7159758d-8337-499e-8b12-e34911f9b4b6>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

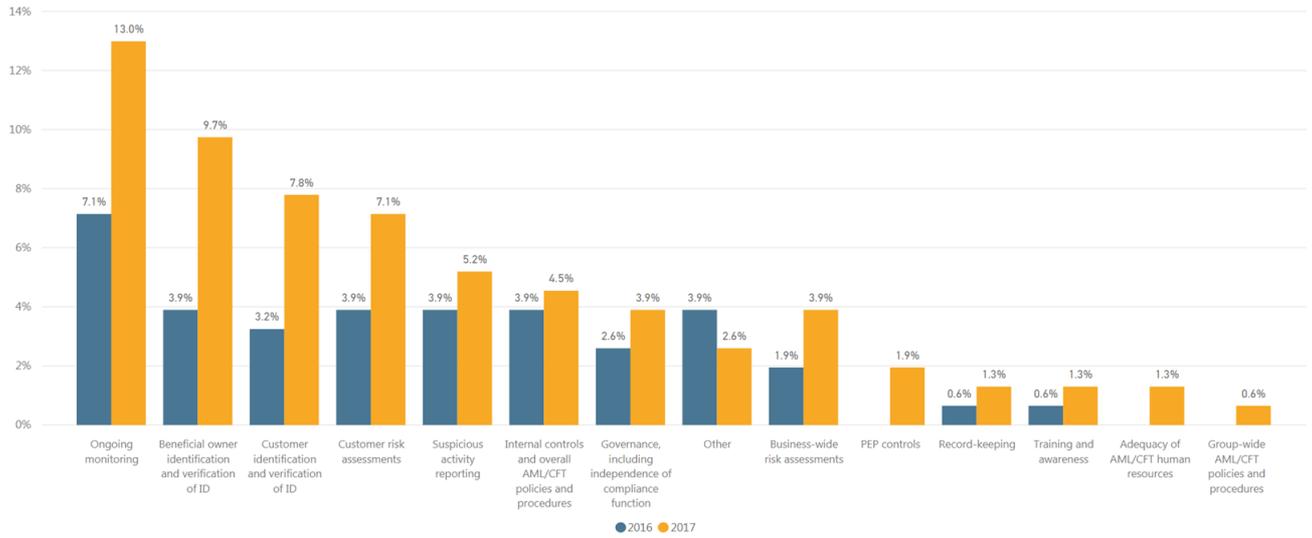


Figure 9: Most common types of breaches in the CI sector — 2016 versus 2017.

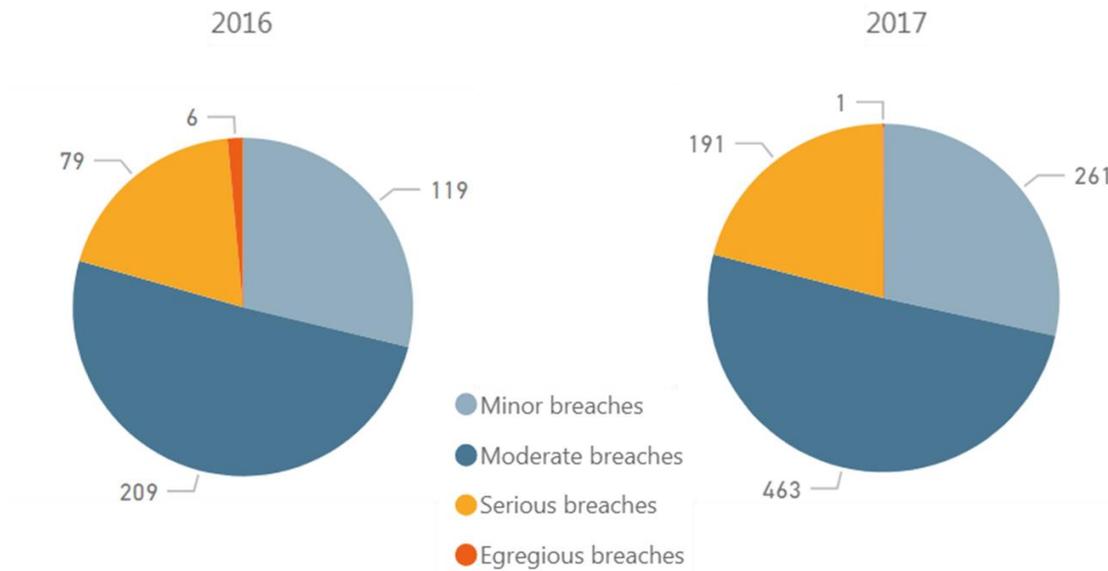


Figure 10: Number of breaches in the CI sector by their seriousness — 2016 versus 2017.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

### III. OVERALL RISK PROFILE OF THE SECTOR

70. After considering inherent risks and controls, the majority of CAs viewed the overall ML/TF risk profile in the CI sector as either significant or moderately significant (see Figure 11 for more details). This classification remained broadly the same in 2016 and 2017. In most cases, it appears that the overall risk rating is the same as the inherent risk rating, leading to the conclusion that, potentially, the controls in place were not sufficient to mitigate the overall risk in the sector.

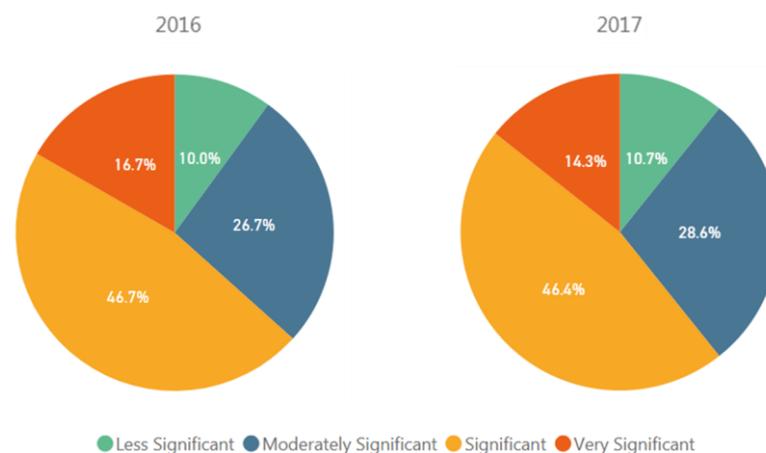


Figure 11: Overall ML/TF risk profile of the credit institution sector — 2016 versus 2017.

### IV. EMERGING RISKS IN THE SECTOR

71. FinTech featured in most responses from the CAs as one of the main current and emerging risks (see section 4.2 above for more details). CAs are also concerned about the increased use of virtual currencies by customers of CIs and the lack of transparency associated with these transactions. In addition, the CAs have identified emerging risks linked with identity theft, potential regulatory loopholes and an increased use of e-commerce services.

### V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

72. From the responses received, it appears that CIs have put in place the required systems and controls, including AML/CFT policies and procedures, but the main concerns that CAs have are



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

related to the effectiveness of these systems and controls when they are applied in practice. To help address these shortcomings, the CAs may consider communicating their expectations about the level of controls expected within the CI sector and how they should be applied.

## 5.2 LIFE INSURANCE UNDERTAKINGS

73. In total, 31 CAs responsible for the supervision of AML/CFT compliance within the life insurance sector provided their responses to the ESAs' questionnaire for 2016; 27 CAs provided their responses in relation to 2017 data.

### I. INHERENT RISKS IN THE SECTOR

74. Traditionally, the life insurance sector's vulnerability to ML/TF has been considered low and the responses received to the ESAs' questionnaire reflect this; they show that the majority of CAs consider the sector to have moderately significant or less significant exposure to ML/TF risks (see Figure 12 for more details). Any differences in the inherent risk rating between CAs can be attributed to the nature and complexity of life insurance products in different Member States. For example, in those Member States where life insurance products linked to investments are widely available, the sector is considered more vulnerable to money laundering.

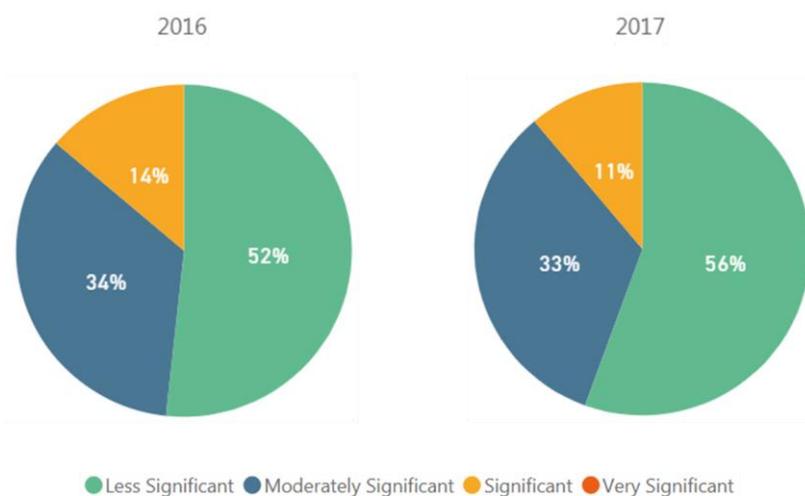


Figure 12: Inherent ML/TF risk profile of the life insurance undertakings — 2016 versus 2017.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

75. The sector in general has very little exposure to cross-border transactions and, from the ML/TF risk point of view, the majority of CAs consider cross-border transactions and activities to present a less significant risk (see Figure 13 for more details).

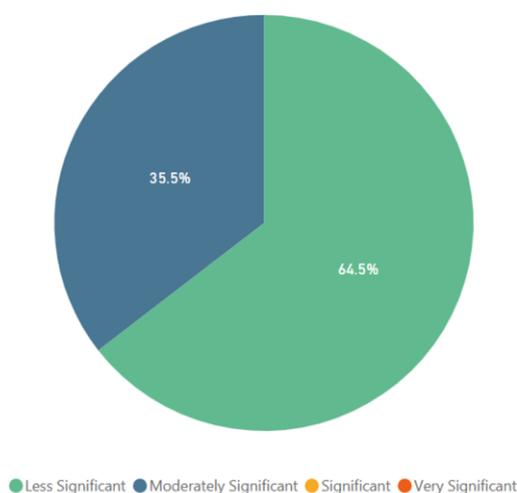


Figure 13: Life insurance undertakings' exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

76. From the responses received, it appears that CAs are generally satisfied with the quality of controls in this sector and have largely rated them as good or very good in both 2016 and 2017 (see Figure 14 for more details). In particular, CAs appear to be satisfied with the quality of controls related to the identification and risk rating of customers, as well as record-keeping practices, in life insurance undertakings (LIUs). In terms of customer identification, the majority of CAs consider the adequacy and effectiveness of policies and procedures put in place by LIUs to be of a sufficiently good level.

77. However, there are a number of areas highlighted by CAs that require improvements. The key areas of concern relate to the quality of business-wide and individual risk assessments, transaction monitoring and the identification and reporting of suspicious transactions, as well as the adequacy of AML/CFT resources. These shortcomings are not mutually exclusive, as LIUs' failure to understand and assess ML/TF risks would have an impact on their ability to implement



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

effective transaction monitoring controls and therefore would have an impact on their ability to identify and report suspicious transactions. The issues regarding the quality of a risk assessment may be explained by the fact that, typically, LIUs have access to less information about the customer than in other sectors because of the low frequency of transactions throughout the business relationship, and the determination of ML/TF risk generally happens at the outset of the relationship. Low transaction frequency, coupled with a low inherent ML/TF risk, may also create an impression that robust transaction monitoring controls are not required in this sector and that suspicious activities can be determined merely on a basis of ‘unusual behaviours’. In addition, the lack of adequate AML/CFT resources might have contributed to these shortcomings.

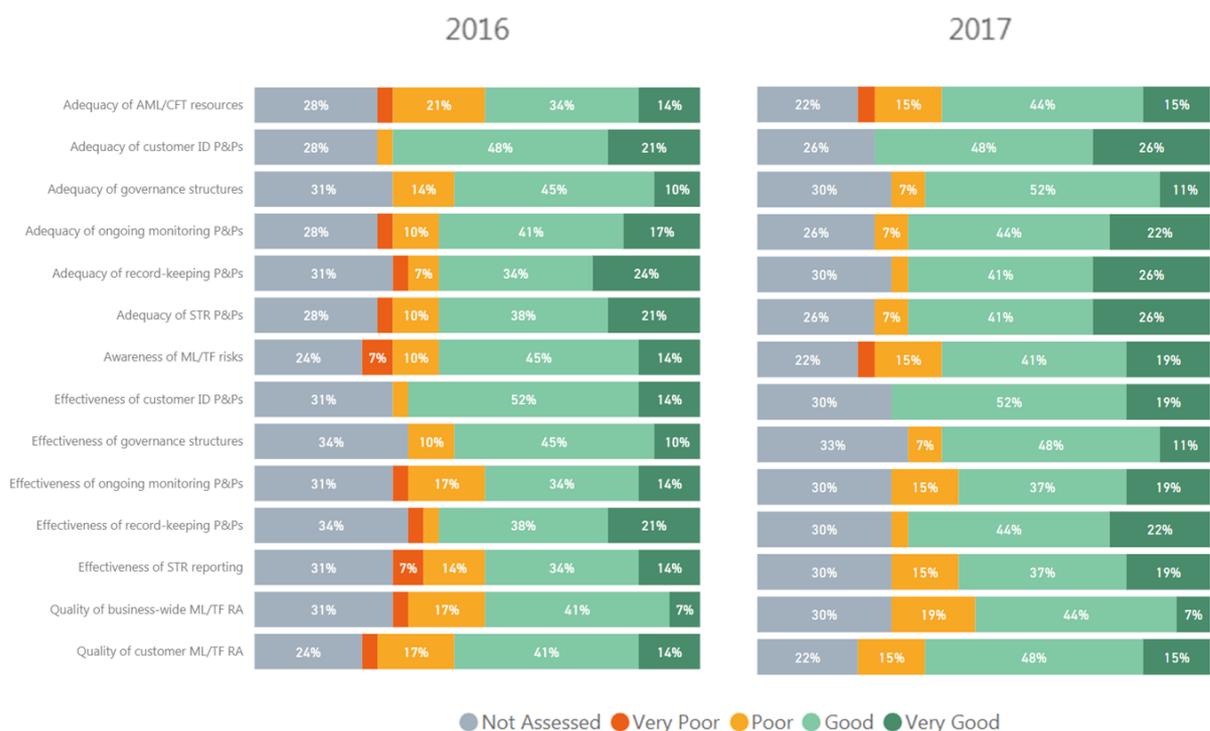


Figure 14: Quality of controls in LIUs — 2016 versus 2017.

78. While supervisory activity has been relatively low owing to the low inherent risk within this sector (see Figures 1 and 2 for more details), the type of breaches that were identified by CAs as a result of their supervisory activities correspond to the controls that CAs are generally concerned about. Commonly, breaches relate to LIUs’ failures to implement sufficient controls



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

for the identification and verification of customers, the assessment ML/TF risks associated with customers and ongoing monitoring (see Figure 15 for more details). The majority of breaches identified are considered minor or moderate (see Figure 16).

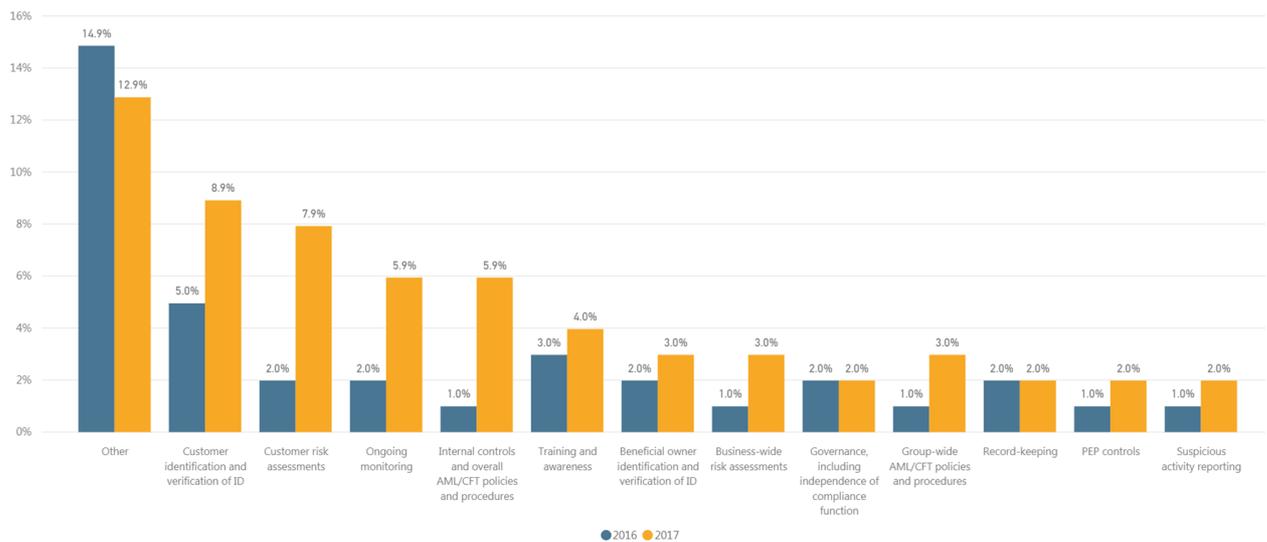


Figure 15: Most common types of breaches identified in the LIUs — 2016 versus 2017.

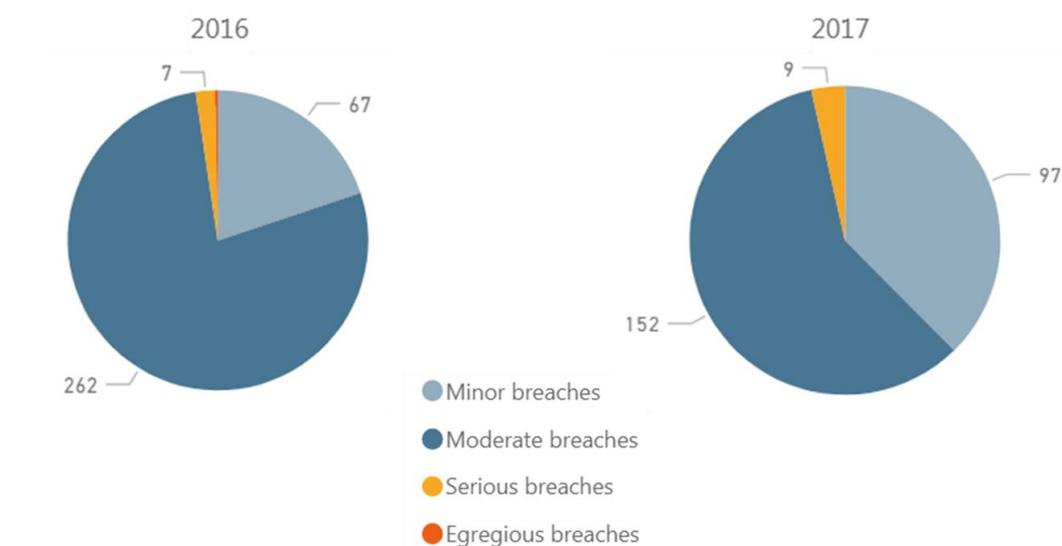


Figure 16: Number of breaches by their seriousness identified in LIUs — 2016 versus 2017.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

### III. OVERALL RISK PROFILE OF THE SECTOR

79. Life insurance products are designed to protect the policy holder financially against the risk of uncertain future events, although some life insurance products can also be bought as investment products or for pension purposes. Most life insurance products are designed for the long term and often will pay out only on a verifiable event, such as death or retirement. When compared with other sectors, life insurance does not provide enough flexibility to be the first choice for ML/TF purposes. Therefore, the majority of CAs consider the sector's overall risk profile as moderately significant or less significant from an ML/TF risk perspective (see Figure 17). Very few CAs consider the sector to present significant risk, but this may be the case in Member States where life insurance is used for investment purposes. Differences in CAs' assessments of LIUs' overall risk profile between 2016 and 2017 stem largely from the different numbers of respondents.

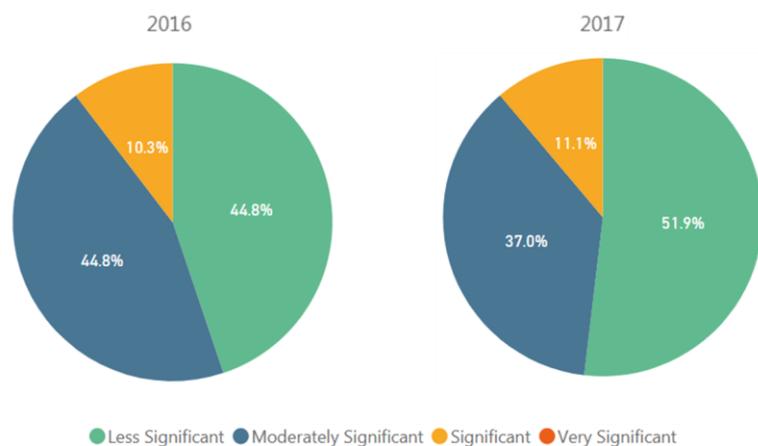


Figure 17: Overall ML/TF risk profile of the LIU sector — 2016 versus 2017.

### IV. EMERGING RISKS IN THE SECTOR

80. As in other sectors, majority of respondents have mentioned the rise in the use of FinTech and RegTech solutions within LIUs as one of the key emerging risks. CAs are generally concerned about the lack of awareness (and sometimes the absence) of AML/CTF regulatory requirements applicable to RegTech solutions and FinTech firms (see subsection 4.2). In addition, the CAs are



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

also concerned about the increased use of web-based insurance platforms and the associated challenges posed by accounts opened without the physical presence of the customer.

## V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

81. The life insurance sector is commonly associated with a low risk of ML/TF by both CAs and the sector itself. This perception, however, could result in the sector being less stringent in its AML/CFT control frameworks. This, coupled with very few supervisory activities within the sector in either 2016 or 2017, which has resulted in a large number of cases in which controls within the sector have not been assessed (see Figure 14), may result in a distorted perception of the overall risk instead of a fair assessment.

82. While the application of the risk-based approach allows the allocation of supervisory resources to areas of higher risk, CAs' failure to supervise a sector effectively means that supervisors will have a limited understanding of the ML/TF risks prevalent in this sector. Therefore, CAs that have not carried out any AML/CFT inspections of the life insurance sector should review their approach to AML/CFT supervision with a view to obtaining sufficient information so that they can be reasonably satisfied that they understand the risks and vulnerabilities in this sector.

83. In addition, CAs should consider if more needs to be done to raise awareness within the sector of both current and emerging risks and the systems and controls they expect LIUs to put in place to mitigate those risks.

### 5.3 LIFE INSURANCE INTERMEDIARIES

84. In total, 28 CAs responsible for supervising the compliance of life insurance intermediaries (LIIs) with AML/CFT rules responded to the ESAs' questionnaire and provided data for 2016 and 24 CAs provided data for 2017.

#### I. INHERENT RISKS IN THE SECTOR

85. The majority of CAs consider the LII sector to have less significant exposure to ML/TF risks (see Figure 18). When compared with the LIUs, the level of inherent ML/TF risk associated with LIIs



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

is lower because often LIIs' responsibilities do not include handling of payments from customers. The ML/TF risk is reduced even more in this sector where the LII is a tied agent.

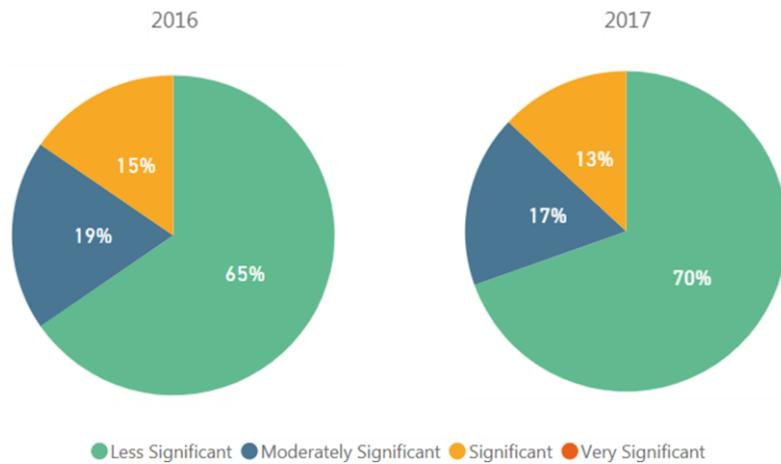


Figure 18: Inherent ML/TF risk profile of LIIs — 2016 versus 2017.

86. This sector's exposure to ML/TF risks arising from cross-border activities is also considered less significant by the majority of CAs (see Figure 19 for more details).

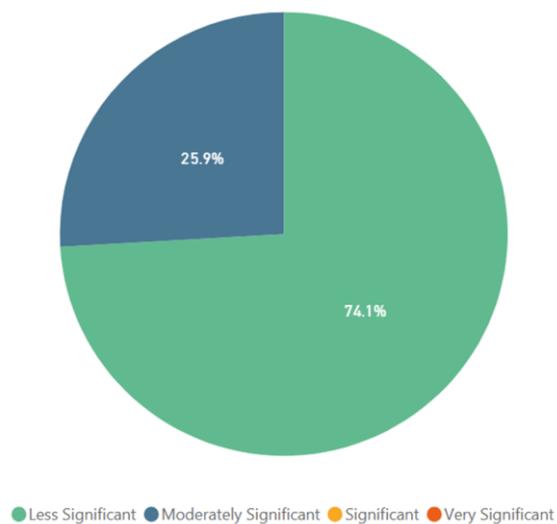


Figure 19: LIIs' exposure to ML/TF risks arising from cross-border activities.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

87. From the responses received to the ESAs' survey, it appears that, when CAs have carried out an assessment of controls, they consider that the controls put in place by LIIs are good or very good (see Figure 20 for more details). However, the responses also highlight that a large number of CAs have not carried out an assessment of controls in this sector, which can be explained by CAs focusing on those sectors that are more exposed to ML/TF risks.

88. Generally, CAs appear to be satisfied with 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, controls relating to the adequacy of ongoing monitoring policies and procedures, the adequacy and effectiveness of STR policies and procedures, and the quality of a business-wide risk assessment have raised some concerns for the CAs.

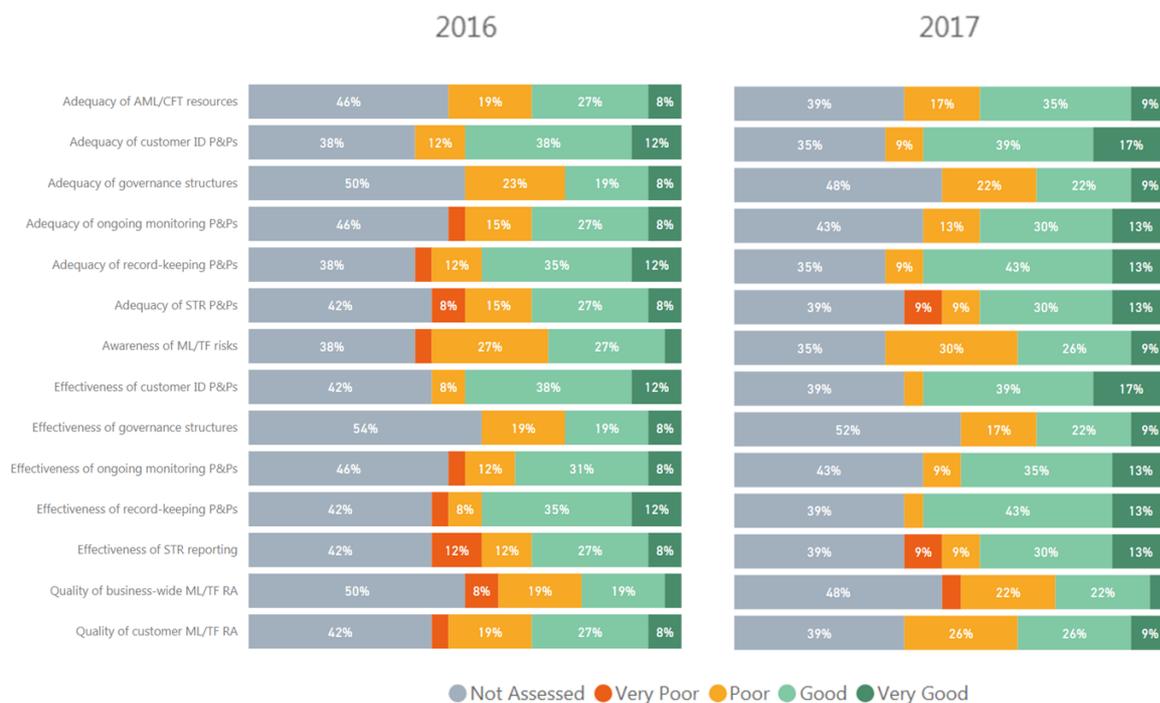


Figure 20: Quality of controls in LIIs — 2016 versus 2017.

89. From the responses received, it appears that only a relatively small number of breaches have been identified in this sector, which may be linked to the relatively low level of supervisory



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

activity in this sector (see Figures 1 and 2). However, most breaches that were identified are classified by CAs as minor or moderate (see Figure 22) and, similarly to LIUs, relate to the identification and verification of customers and the assessment of ML/TF risks associated with them (see Figure 21 for more details).

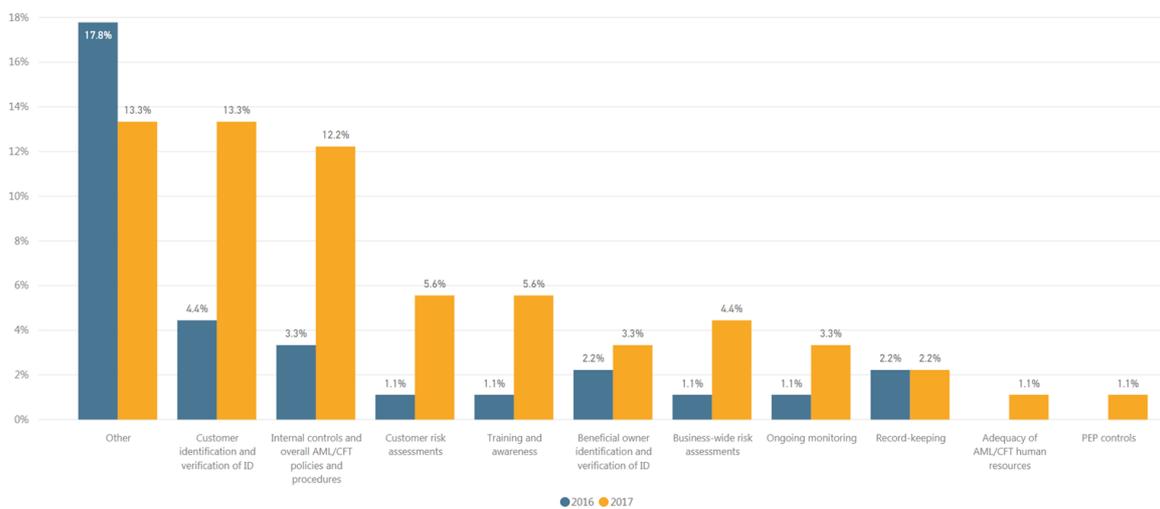


Figure 21: Most common types of breaches identified in LIIs — 2016 versus 2017.

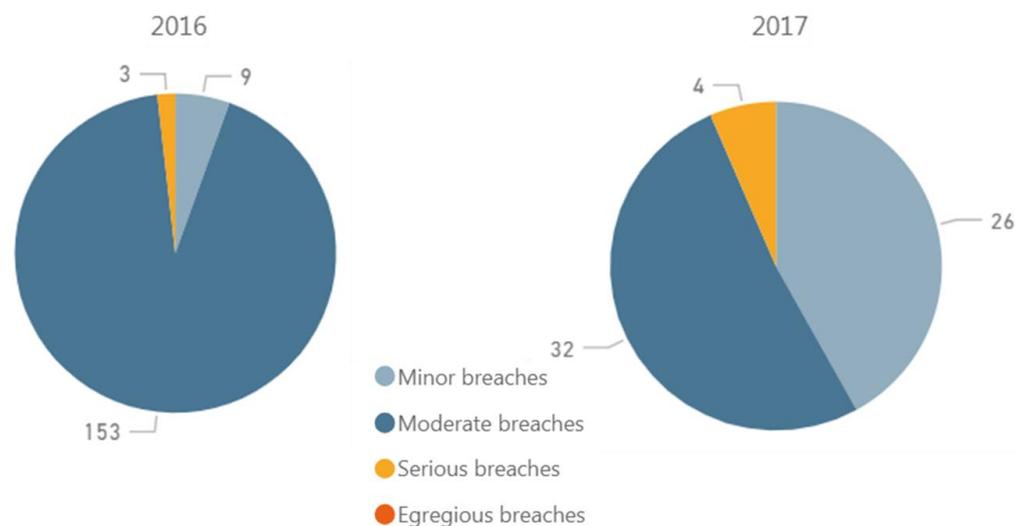


Figure 22: Number of breaches by their seriousness identified in LIIs — 2016 versus 2017.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

### III. OVERALL RISK PROFILE OF THE SECTOR

90. The overall risk profile of the LII sector has been classified as a less significant risk by the majority of CAs (see Figure 23). From the responses received, it is evident that CAs are concerned about the levels of training provided to the staff in this sector and consider the level of training to be inadequate. This can be explained by the lack of understanding and prioritisation of ML/TF risks by the senior management in this sector. CAs have also identified weaknesses in the controls framework related to the identification of customers, beneficial owners and beneficiaries, which increase the risk profile of the sector.

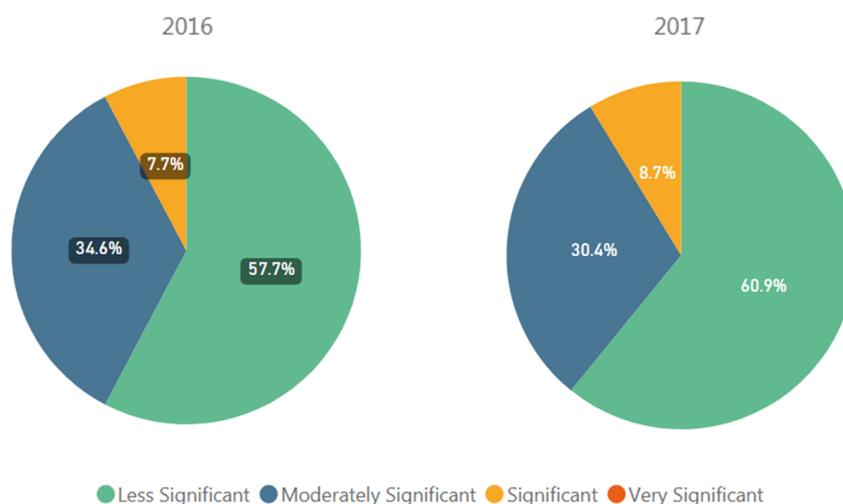


Figure 23: Overall ML/TF risk profile of the LII sector — 2016 versus 2017.

### IV. EMERGING RISKS IN THE SECTOR

91. Responses to the questionnaire highlight that CAs have identified emerging risks for this sector in three areas: delivery channels, geographical risk and legislative changes. Delivery channels are likely to pose an ML/TF risk in situations when the number of intermediaries is unusually large or when on-boarding of customers is carried out through the group or an off-shore company. As regards geographical risk, CAs are concerned about risks associated with LIIs established in high-risk countries, which may then attract prospective customers from those high-risk jurisdictions.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

92. Owing to its nature, this sector is considered low risk for ML/TF purposes, which explains the low levels of supervisory activity in this sector. While, in line with the risk-based approach, the CAs are required to focus their supervision on more risky areas and sectors, they are also required to have a good understanding of ML/TF risks present in all sectors, including those presenting a low risk of ML/TF. Considering the low levels of supervisory activities and the large proportion of CAs that have not carried out an assessment of controls in this sector, the question arises of whether or not the CAs' understanding of the overall risk profile of this sector is sufficiently informed. Therefore, CAs that have not carried out any AML/CFT inspections of the LII sector should review their approach to AML/CFT supervision with a view to obtaining sufficient information so that they can be reasonably satisfied that they understand the risks and vulnerabilities in this sector.

### 5.4 E-MONEY ISSUERS

93. In total, 31 CAs responsible for supervising the compliance of e-money issuers (EMIs) with AML/CFT rules responded to the ESAs' questionnaire in relation to 2016 data, and 28 CAs responded in relation to 2017.

94. In addition, in September 2018, the ESAs organised a workshop that brought together representatives of CAs, the industry and law enforcement. This workshop aimed to consolidate AML/CFT supervisors' understanding of e-money, the ML/TF risk associated with e-money products and business models, and the AML/CFT systems and controls that EMIs put in place to mitigate those risks.

## I. INHERENT RISKS IN THE SECTOR

95. The level of inherent ML/TF risk associated with the EMI sector depends primarily on the features of individual e-money products and the degree to which e-money issuer EMIs use other persons to distribute and redeem e-money on their behalf. Specifically:



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

- (i) Risk inherent in product design is determined primarily by the utility and negotiability of the e-money product: the more closely the product resembles banking products, the higher the ML/TF risk will be. By contrast, the risk is reduced if the product places restrictions on its use. Examples of restrictions include certain value and transaction thresholds, no ATM cash withdrawal facilities, acceptance limited to a small number of merchants only, no person-to-person transfers and no cross-border facilities<sup>29</sup>.
- (ii) Risk inherent in distribution models is determined primarily by the extent to which e-money is distributed by persons other than the EMI. The greater the number of persons involved in the distribution chain, the more reduced the issuer's oversight is likely to be.

96. In some situations in which the ML/TF risk is demonstrably low, EMIs can benefit from exemptions from certain CDD measures<sup>30</sup>. The European Commission, taking note of the perceived level of anonymity resulting from the application of these exemptions, therefore described the level of inherent ML/TF risk associated with e-money as significant or very significant in its 2017 SNRA<sup>31</sup>.

97. Feedback from stakeholders suggests that only a very small proportion of e-money products are truly anonymous. In most cases, in the absence of formal identification and verification requirements, the use of technology or the imposition of specific requirements, such as requiring payments to originate from the customer's account with a credit or financial institution, enables firms to link customers to transactions on the basis of other identifiers. These processes appear to generate sufficient meaningful information to support law enforcement agencies' investigations.

98. Nonetheless, like other financial products, there is evidence to suggest that e-money products have been abused for ML/TF purposes. Most CAs therefore assessed the inherent ML/TF risk

---

<sup>29</sup> See Chapter 3 of Title III of the risk factors guidelines.

<sup>30</sup> Article 12 of the AMLD and AMLD3's Simplified Due Diligence provisions provide for exemptions from certain CDD obligations subject to specific conditions.

<sup>31</sup> European Commission's Supra National Risk Assessment; published on 26 June 2017; available at: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=81272](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272)



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

associated with this sector was significant or moderately significant throughout both 2016 and 2017 (see Figure 24 for more details).

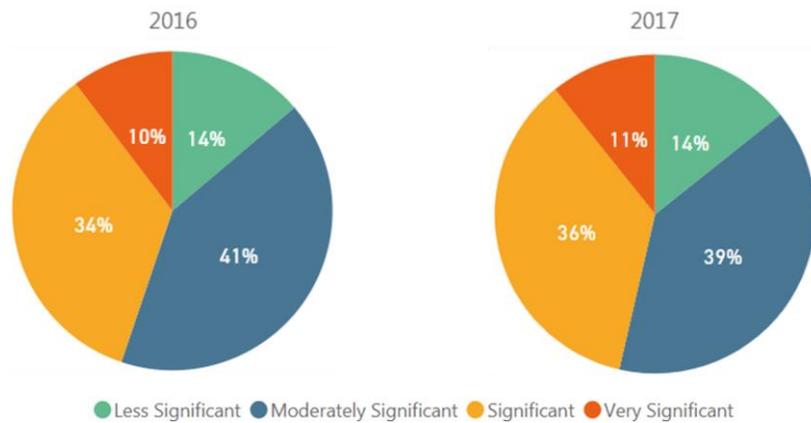


Figure 24: Inherent ML/TF risk profile of the e-money sector — 2016 versus 2017.

99. This sector's exposure to ML/TF risks arising from cross-border activities is considered moderately significant or significant by the majority of CAs (see Figure 25 for more details).

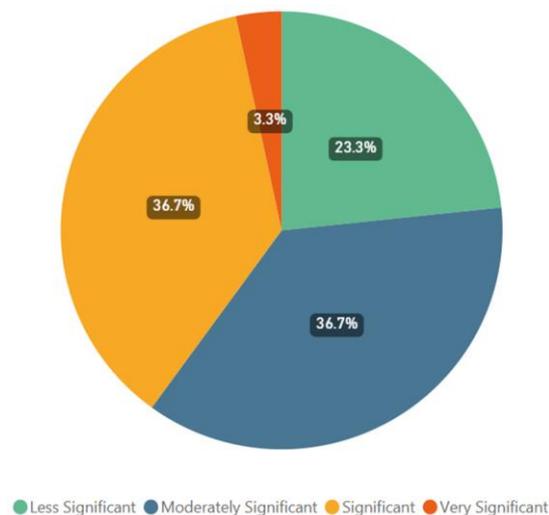


Figure 25: E-money sector's exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

100. There was wide variety in how CAs assessed this sector's risk mitigation, from good to very poor (see Figure 26 for more details). Feedback from CAs suggests that this could be due to the



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

relative maturity of the sector in each Member State, the nature of inspections (e.g. thematic reviews of a randomly selected sample of firms versus inspections triggered by specific concerns), the number of inspections or a combination thereof. Where breaches were identified, these were mostly minor or moderate, with serious or egregious breaches identified in only four cases (see Figures 27 and 28 for more details).

101. In particular, CAs identified weaknesses in relation to the adequacy and effectiveness of ongoing monitoring policies and procedures, awareness of ML/TF risks and the effectiveness of STRs and governance arrangements. This is of concern in a sector that, owing to the technology-driven nature of many of its products, relies heavily on transaction monitoring as a risk mitigation tool and where risk is driven by the extent to which issuers can exert effective oversight over their distributor networks.

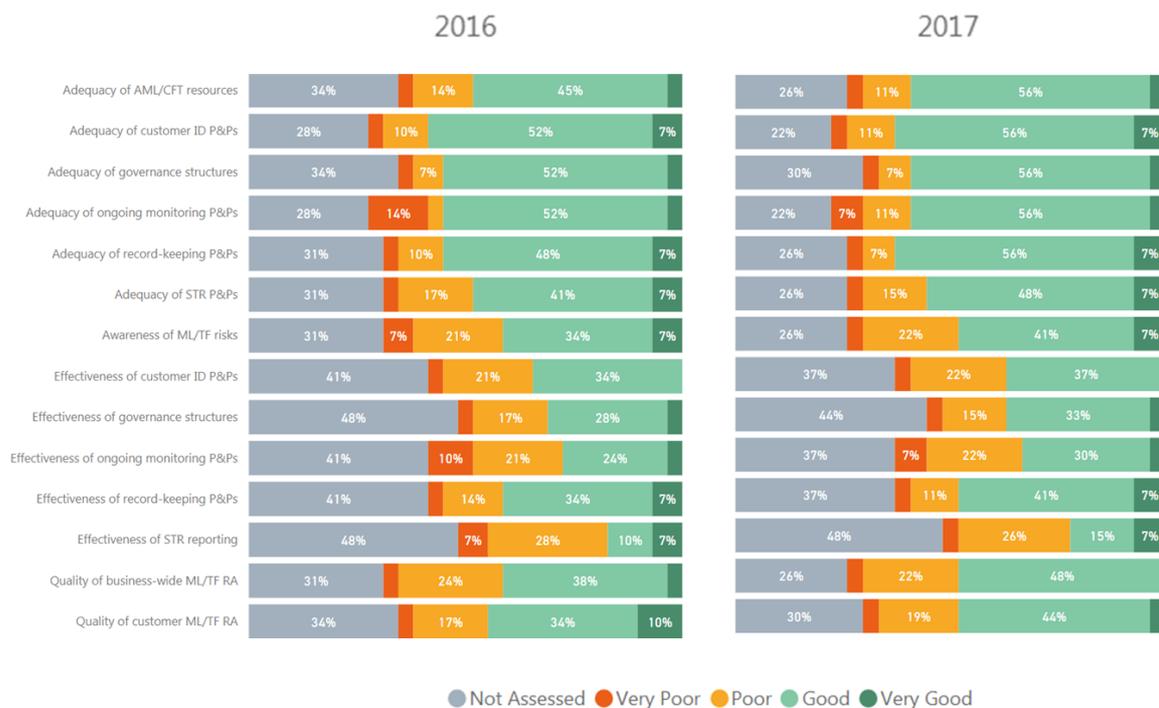


Figure 26: Quality of controls in the e-money sector — 2016 versus 2017.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

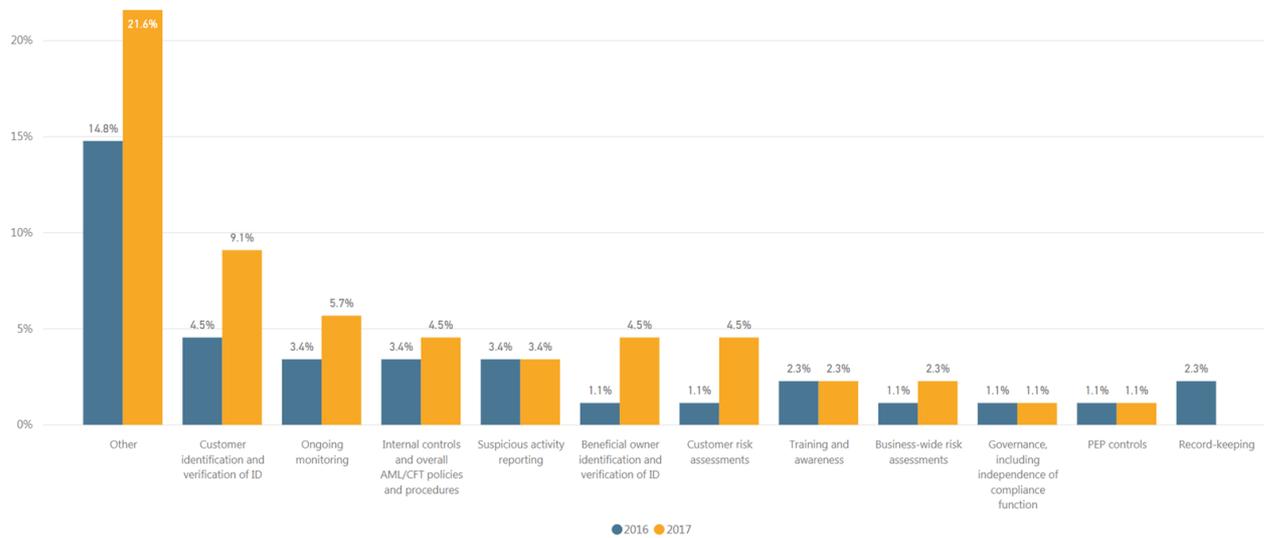


Figure 27: Most common types of breaches in the e-money sector — 2016 versus 2017.

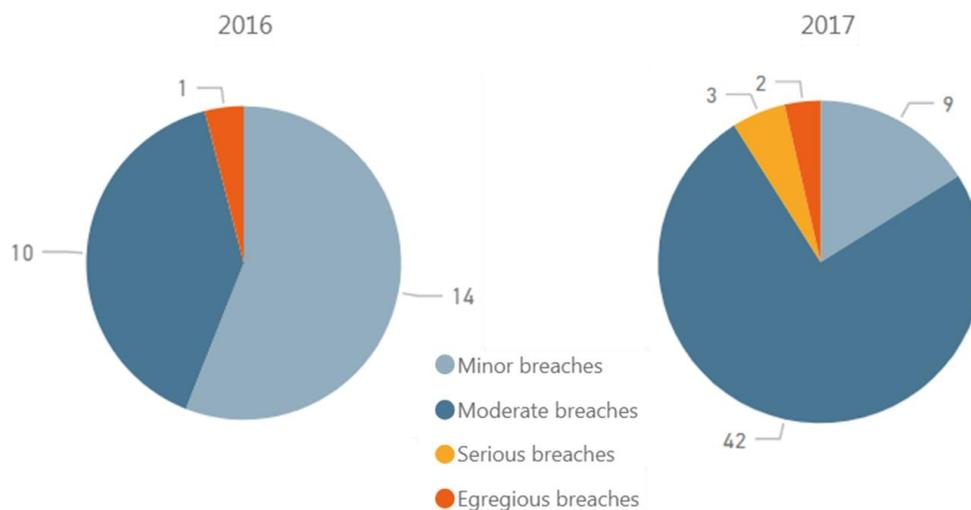


Figure 28: Number of breaches by their seriousness identified in the e-money sector — 2016 versus 2017.

### III. OVERALL RISK PROFILE OF THE SECTOR

102. From the responses received, it appears that most CAs have assessed the sector's overall risk profile as moderately significant or significant (see Figure 29). In contrast, a significant proportion of firms in the e-money sector view their sector's overall ML/TF risk profile as less significant or moderately significant. The difference in perception stems mainly from divergent



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

views of the extent to which EMIs' AML/CFT controls are effective and sufficiently robust to mitigate the significant inherent ML/TF risks that the sector is exposed to.

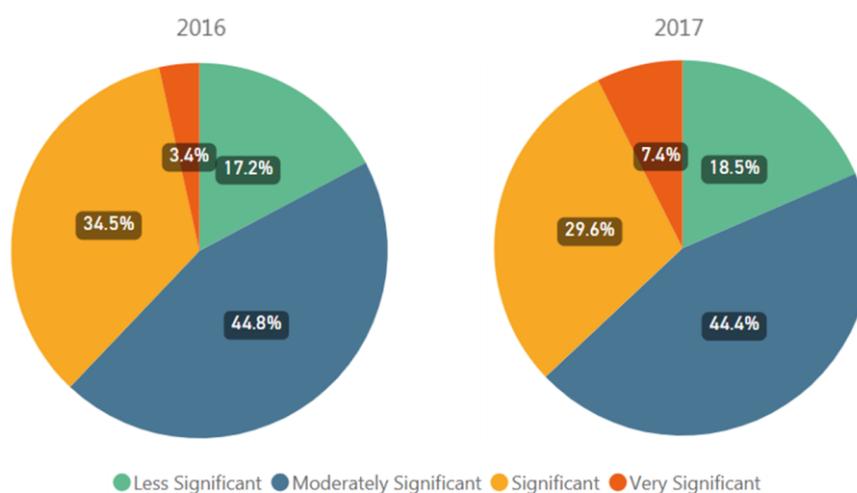


Figure 29: Overall ML/TF risk profile of the e-money sector — 2016 versus 2017.

#### IV. EMERGING RISKS IN THE SECTOR

103. Overall, the emerging risks identified by CAs do not describe new developments but rather reveal the specific shortcomings and deficiencies identified in the sector in each Member State. However, like in other sectors, many CAs also pointed to emerging risks in relation to FinTech, including remote on-boarding applications and virtual currencies, which is of particular importance in a sector that is already very technology driven.

#### V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

104. It is recommended that CAs should:

- carry out a risk assessment of this sector, clearly identifying and assessing all ML/TF risk factors on the basis of various sources of information available to them, including engagement with industry representatives;
- carry out targeted inspections, for example thematic reviews, in areas in which they do not have sufficient information available to carry out a sufficiently robust risk assessment of the



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

sector, so they can develop a better understanding of the sector and the type and quality of controls applied by EMI, with particular focus on transaction monitoring;

- ensure that EMIs' risk assessments cover all types of customers and that their policies and procedures define what type of CDD should be applied for each risk category, with clear provisions explaining when and how to perform enhanced CDD. In addition, CAs should be satisfied that EMIs employ appropriately skilled staff and provide them with training specifically tailored to address risks particularly present in the e-money sector;
- provide the sector with appropriate guidance setting out their regulatory expectations.

## 5.5 PAYMENT INSTITUTIONS

105. The ESAs received responses from 32 CAs responsible for the AML/CFT supervision of payment institutions (PIs) in respect of 2016 and from 28 CAs in respect of 2017.

106. In addition, in September 2018, the ESAs organised a workshop on money remitters, which brought together representatives of CAs, the industry and law enforcement. This workshop aimed to consolidate AML/CFT supervisors' understanding of the ML/TF risk associated with money remittance and the AML/CFT systems and controls that money remitters have put in place to mitigate those risks.

### I. INHERENT RISKS IN THE SECTOR

107. The majority of CAs considered that the inherent ML/TF risk profile of PIs was either significant or very significant (see Figure 30 for more details). This overall rating is also reflected in the ratings of separate risk factors, for which products and services represented a marginally higher proportion of significant risk or very significant risk but, in general, similarly high risk ratings were given to each risk factor.

108. The ML/TF risk attached to PIs' activities varies considerably depending on the services provided and the customer type. The most significant ML/TF risk relates to PIs that offer money remittance services, owing to the cash-intensive nature of their services, high speed and/or high volumes of transfers (albeit transfer size is typically small) and transfers to high-risk jurisdictions.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

The risks are significantly higher when PIS' business models are based on the use of an agent network owing to the potential for collusion between the agents and criminals. These risks are also emphasised by a number of CAs, which have published reports based on thematic reviews carried out by them, and in the SNRA published by the European Commission.

109. The significant level of ML/TF risk associated with the sector appears to have led firms, in particular banks, to adopt 'de-risking' policies towards customers who provide money remittance services in certain higher risk regions. This trend raises concerns among CAs, as de-risking may ultimately lead to money remittance services being driven underground (see subsection 4.8 on de-risking for more details). Financial inclusion concerns also arise, as money remittance services play an important role for customers who have limited or no access to other regulated financial services.

110. At the recent workshop on money remitters organised by the ESAs, CAs and law enforcement agencies indicated continued evidence of the use of hawala<sup>32</sup> for ML/TF purposes, in particular for TF purposes, where small-scale money transfers can be used to finance high-impact attacks. CAs cite difficulties detecting unauthorised hawala, as it typically maintains no public presence.

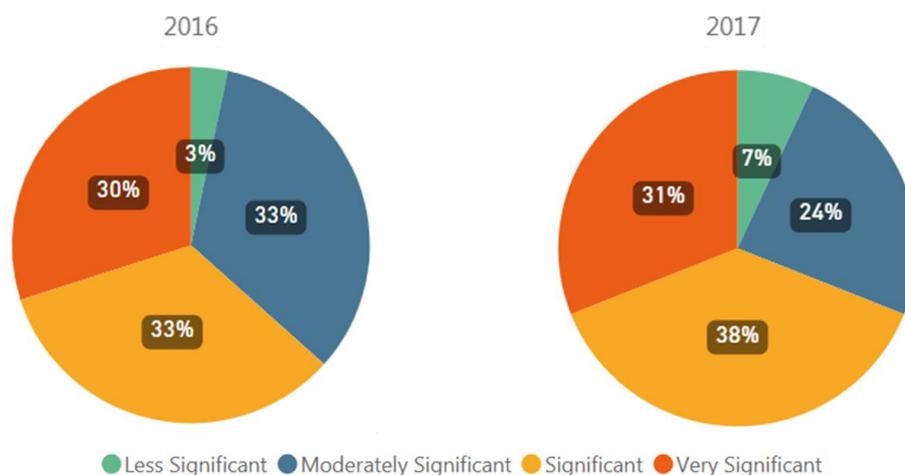


Figure 30: Inherent ML/TF risk profile of the PI sector — 2016 versus 2017.

<sup>32</sup> For the purposes of this Joint Opinion, 'hawala' means informal transfers of funds without the involvement of authorised firms.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

111. The sector is highlighted by CAs as being particularly vulnerable to cross-border activities linked to terrorist financing. Investigations carried out by law enforcement agencies following recent terrorist attacks, for example in Paris and the UK, have confirmed that terrorists have used money remittance services to raise and move funds. Therefore, the sector's exposure to ML/TF risks arising from cross-border activities is rated as significant or very significant by the majority of CAs (see Figure 31 for more details).

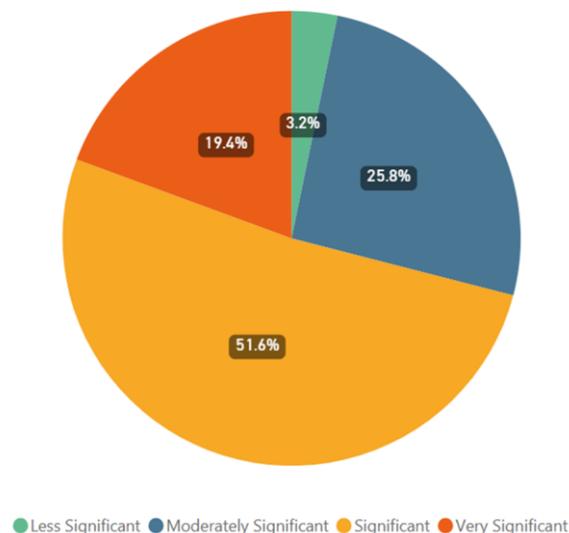


Figure 31: PIs' exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

112. There is almost an even split between good, poor and very poor ratings of controls in both 2017 and 2016. Only a small minority of CAs rated the overall quality of controls as being very good in either year (see Figure 32 for more details). From the responses received, it appears that CAs are satisfied with the adequacy of policies and procedures relating to customer identification and verification, record-keeping and STRs. However, many CAs have raised concerns about the effectiveness of these policies and procedures. CAs are also concerned about the sector's awareness of ML/TF risks, which has resulted in the sector's failure to carry out adequate customer and business-wide risk assessments. These failures raise particular concerns, as the sector's main activity is based on the swift processing of transactions. As such,



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

the main emphasis within the sector should be on controls related to transaction monitoring and reporting of suspicious transactions.

113. From the responses received to the ESAs' survey and the feedback received as part of the ESA workshop, it appears that the CAs are generally concerned about the quality of controls in this sector, particularly those controls relating to the risks associated with the agent networks. CAs consider these controls to be particularly weak in relation to governance arrangements and oversight, as well as the risk awareness and training provided to the agents by PIs.

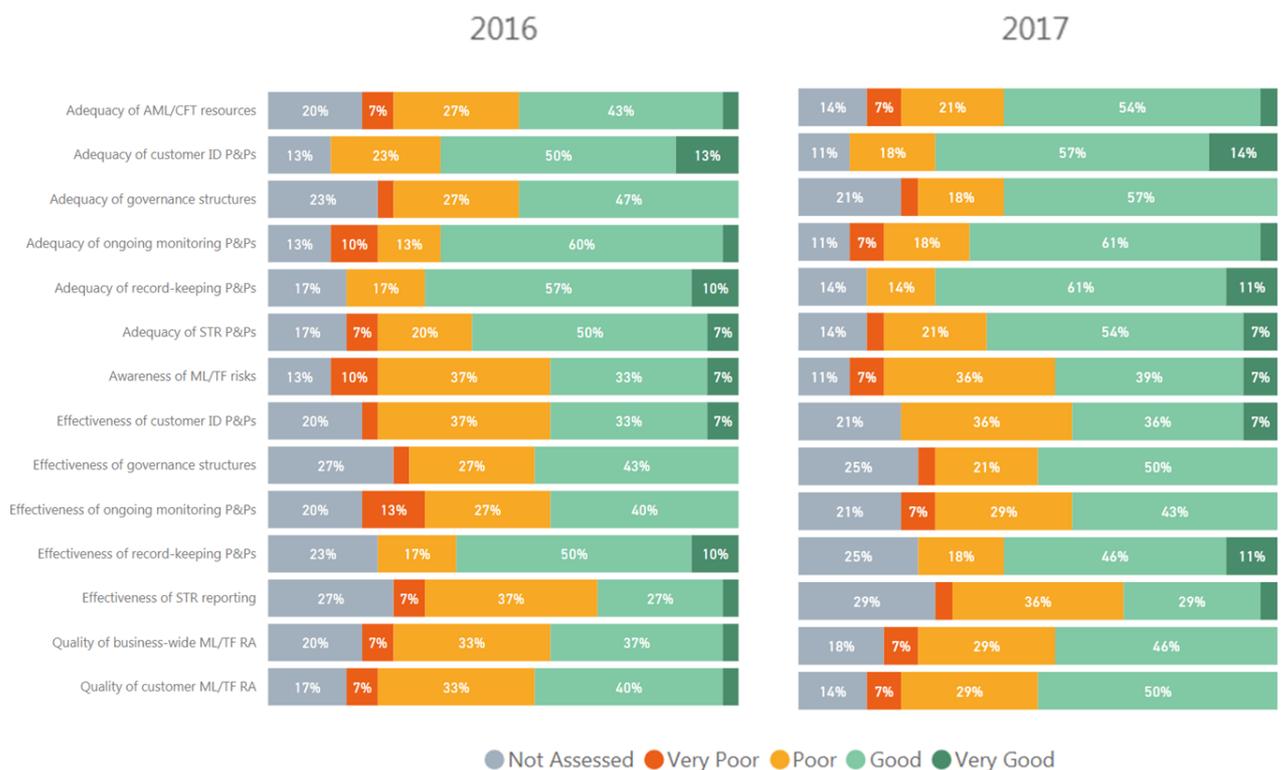


Figure 32: Quality of controls in the PI sector — 2016 versus 2017.

114. When breaches were identified as a result of supervisory activities, they related to the identification and verification of customers and their risk assessments, as well as internal controls failures and ongoing monitoring (see Figure 33). From the responses received, it is evident that a variety of breaches were identified, ranging from minor to egregious (see Figure 34 for more details).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

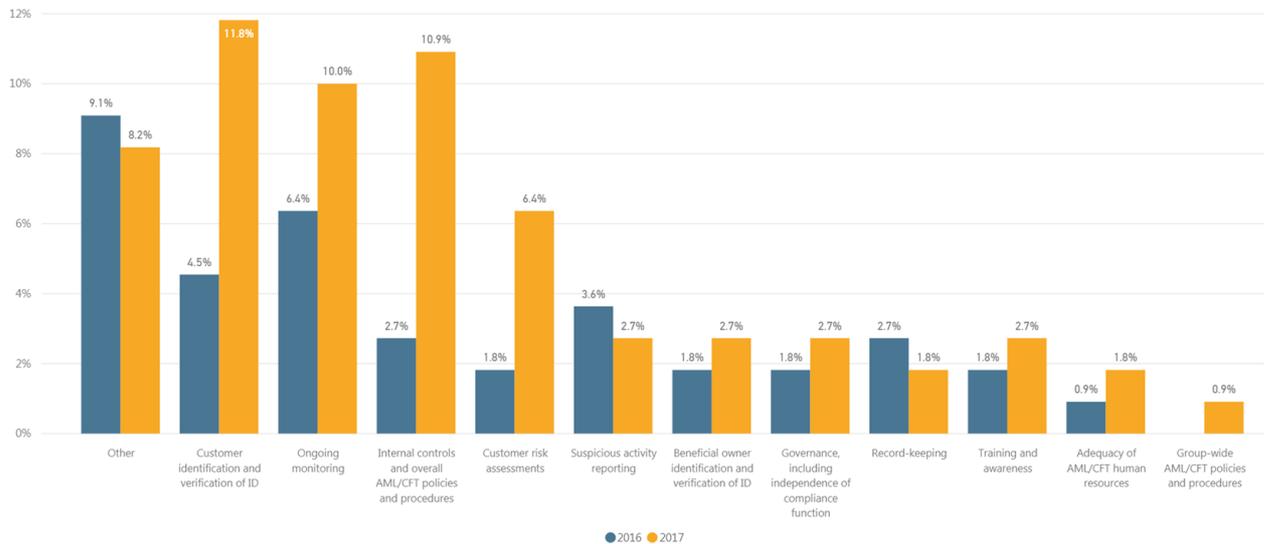


Figure 33: Most common types of breaches in the PI sector — 2016 versus 2017.

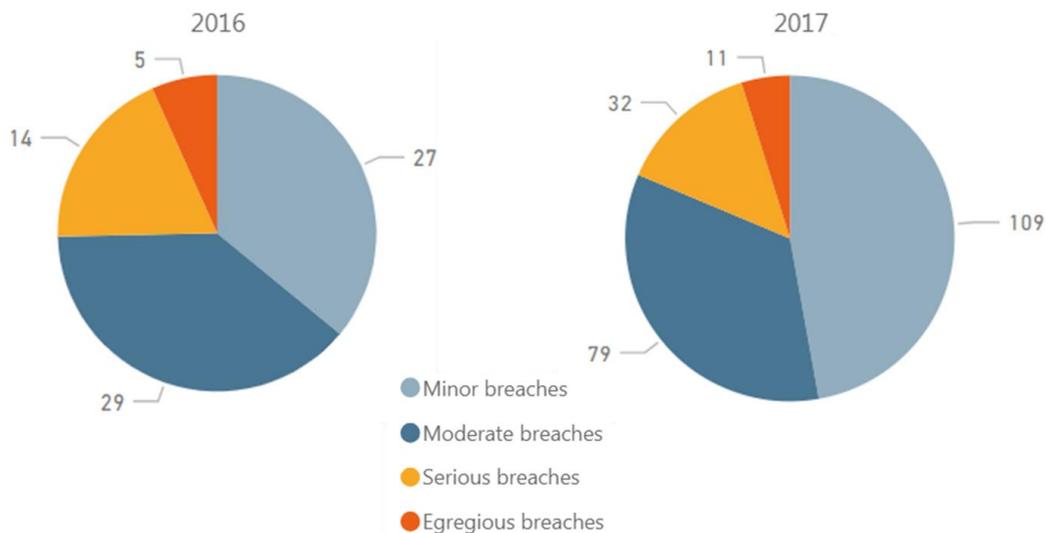


Figure 34: Number of breaches by their seriousness identified in the PI sector— 2016 versus 2017.

### III. OVERALL RISK PROFILE OF THE SECTOR

115. From the responses received, the majority of CAs rated the sector as either significant or very significant from an ML/TF risk perspective (see Figure 35 for more details). This view was particularly shared by those CAs that supervised the highest numbers of PIs within the EU. In contrast, the industry representatives' perception of ML/TF risks in the sector is 'medium' owing



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

to sophisticated transaction monitoring and agent oversight systems and controls put in place by firms. However, the workshop also highlighted that controls may differ significantly between small and large players in the market.

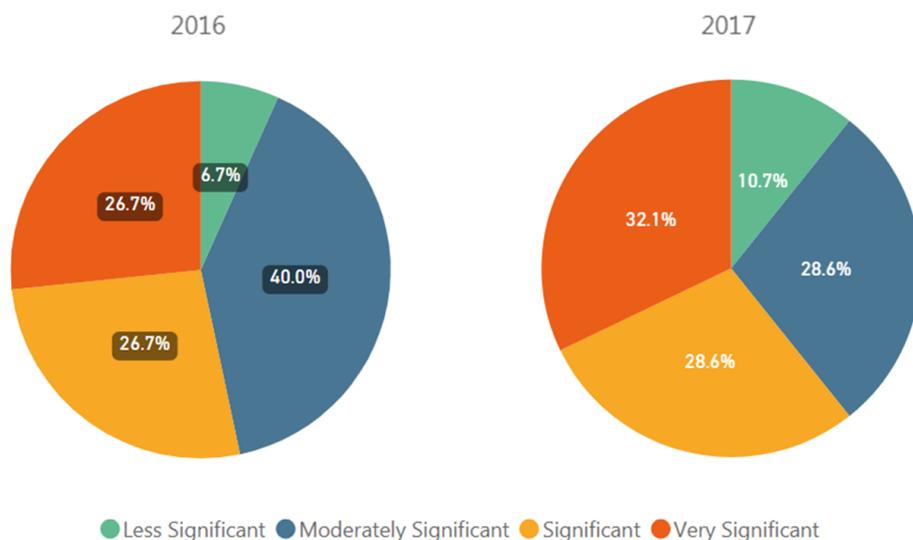


Figure 35: Overall ML/TF risk profile of the PI sector — 2016 versus 2017.

#### IV. EMERGING RISKS IN THE SECTOR

116. The potential misuse of new technologies such as mobile payments to facilitate peer-to-peer money transfers was commonly cited as an emerging risk. Other emerging risks include the introduction of RegTech solutions for customer identification (see subsection 4.2 on new technologies for more details).

#### v. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

117. The concerns raised by CAs about the effectiveness of certain controls and divergent perceptions of ML/TF risks within the sector by industry indicate that further engagement by CAs with the sector is needed. CAs should assess if they have sufficient information available to them, considering that the supervisory activities were relatively low in this sector, to carry out a proper risk assessment of this sector. Similarly, identification and remediation of deficiencies relating to agent oversight should also be an area of priority for supervisory engagement.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

118. De-risking may ultimately lead to money remittance services being driven underground. Consideration should be given to possible outreach and communication to address the de-risking by firms (in particular credit institutions) of their money remittance customers.

## 5.6 CREDIT PROVIDERS (OTHER THAN CREDIT INSTITUTIONS)

119. The ESAs received responses from 23 CAs responsible for the AML/CFT supervision of credit providers (CPs) in respect of 2016 and from 20 CAs in respect of 2017.

### I. INHERENT RISK IN THE SECTOR

120. This sector includes firms of various kinds, offering very different types of products and services, and thus the firms are exposed to different levels of ML/TF risks. The key differences include:

- Consumer CPs often operate through credit intermediaries, with few direct contacts with their customers, and therefore face risks deriving from poor-quality CDD and low levels of ongoing monitoring.
- Factoring, leasing and commercial CPs have completely different operational models and serve different types of customers (trading companies, import/export) and therefore are more exposed to trade-based money laundering, in which commercial trade might become a conduit of illegal funds.

121. The overall level of inherent ML/TF risk of the sector is most frequently considered to be moderately significant or less significant, with only a few CAs considering that the level of inherent risk was significant or very significant (see Figure 36). Contributing to this assessment are the CAs' concerns about the sector's vulnerability to fraud, including online and credit card fraud and mule accounts. The risk in this sector is also increased when credit intermediaries are used by CPs to distribute their products and services. This sector is also vulnerable to being used for terrorist financing purposes, as small amounts of credit can be obtained to finance an act of terrorism. Over- or under-invoicing, in order to create inflated payments and triangulated trade operations that might be aimed at disguising the true destination of funds through the



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

interposition of false beneficiaries, is also considered a risk associated with this sector by some CAs.

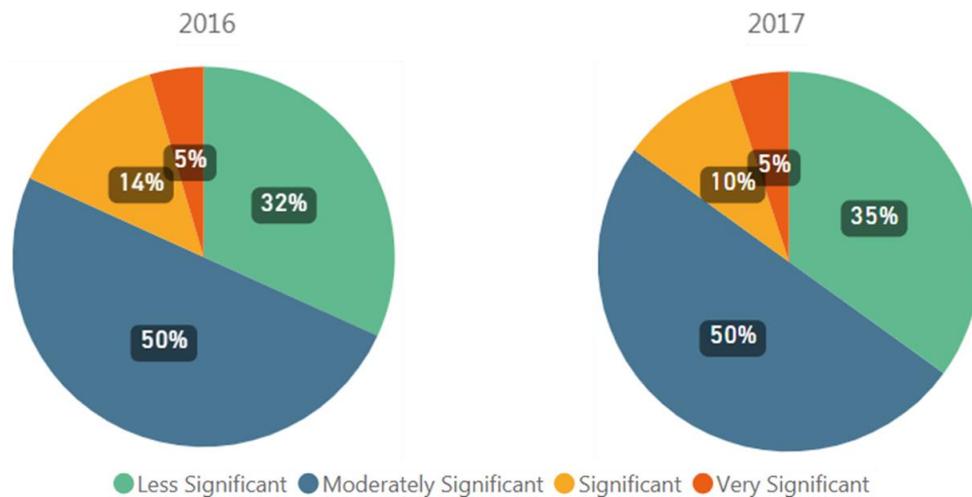
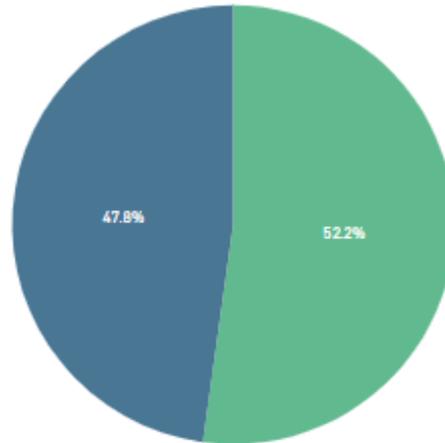


Figure 36: Inherent ML/TF risk profile of the CPs' sector — 2016 versus 2017.

122. From the responses received, it appears that the CAs do not consider this sector to be vulnerable to ML/TF as a result of cross-border activities. This could be attributed to the fact that products and services provided by CPs are generally designed for the domestic market; however, the risk is increased owing to the risk of terrorism financing, which often has a cross-border element to it. Overall, the CAs have rated the cross-border exposure of this sector as less significant or moderately significant (see Figure 37 for more details).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES



● Less Significant ● Moderately Significant ● Significant ● Very Significant

Figure 37: CPs' exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

123. From the responses received, it is evident that CAs are largely satisfied with the quality of risk-mitigating measures in this sector and found them to be good and very good, particularly controls related to the adequacy and effectiveness of customer identification and record-keeping policies and procedures. In contrast, CAs have raised concerns about the adequacy and effectiveness of the ongoing monitoring and STR policies and procedures and, on a number of occasions, have rated them as poor or very poor. In addition, CAs are also concerned about the quality of customers' risk assessments and the awareness of ML/TF risks, which have been rated as poor by a significant proportion of the CAs (see Figure 38 for more details on controls).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

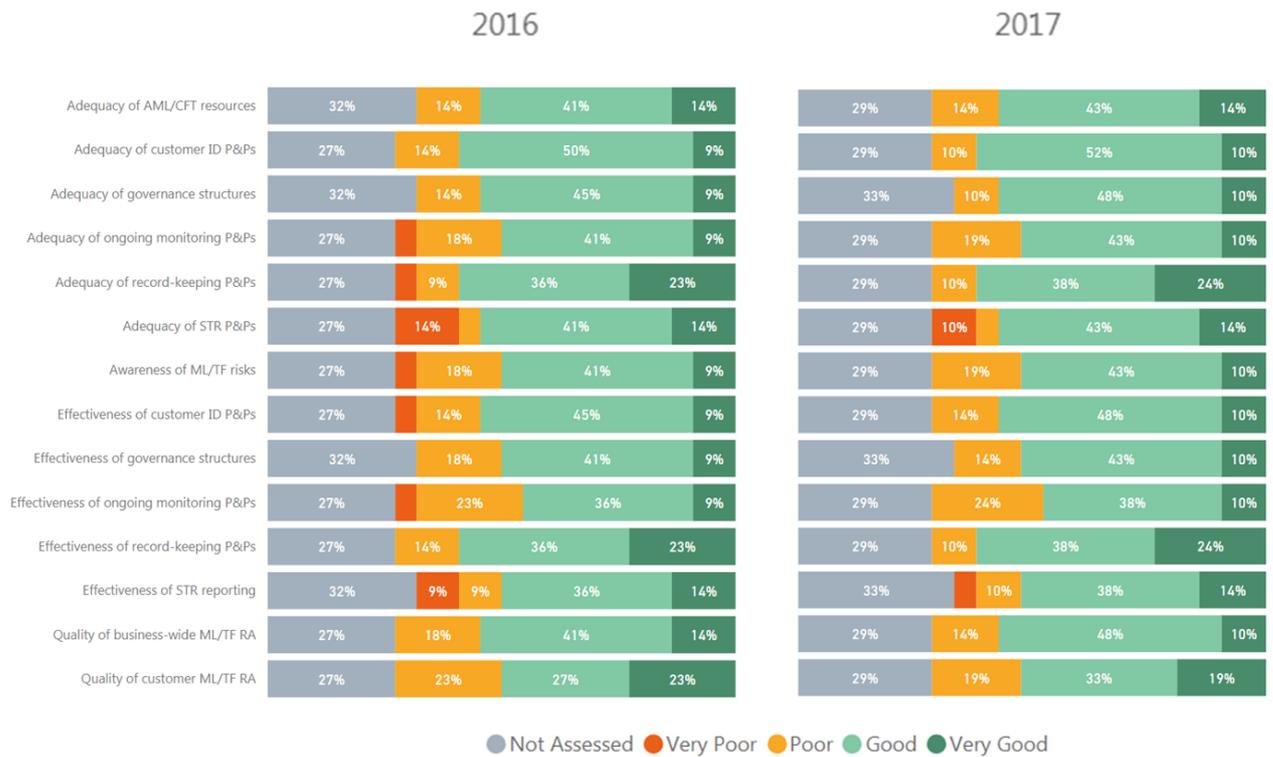


Figure 38: Quality of controls in the CPs' sector — 2016 versus 2017.

124. From the responses received, it appears that, most commonly, breaches of legislation were related to the identification and verification of customers and beneficial owners, as well as weaknesses in internal controls (see Figure 39 for more details). However, most of the breaches identified were classified as minor or moderate and there were no egregious breaches identified in the sector in 2017 (see Figure 40).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

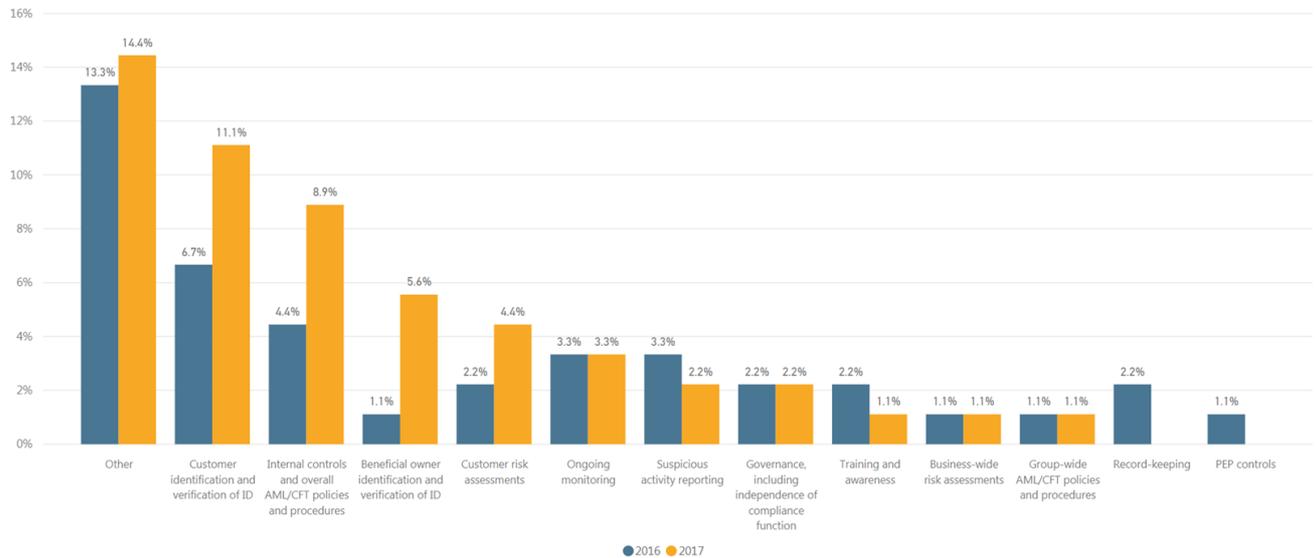


Figure 39: Most common types of breaches in the CPs' sector — 2016 versus 2017.

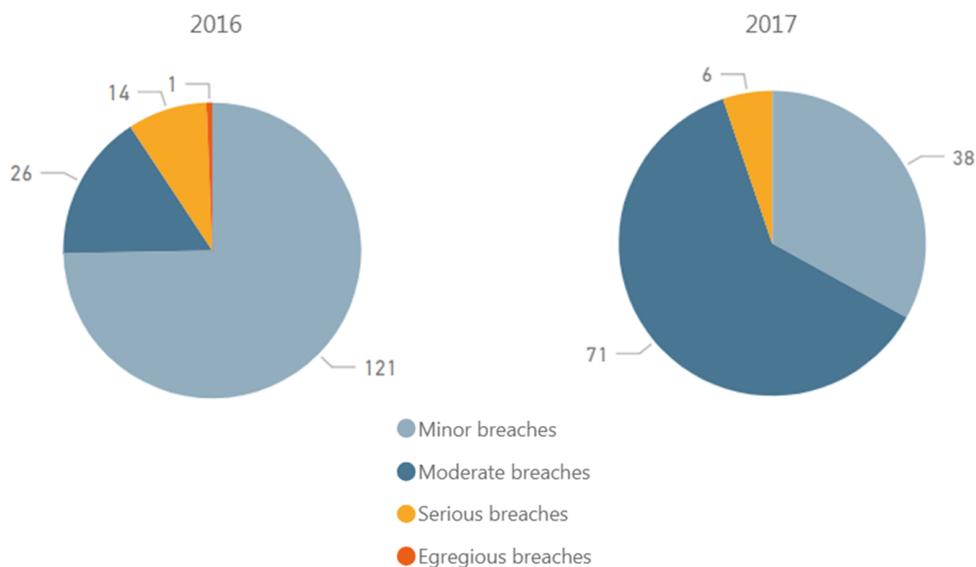


Figure 40: Number of breaches by their seriousness identified in the CPs' sector — 2016 versus 2017.

### III. OVERALL RISK PROFILE OF THE SECTOR

125. The majority of CAs consider this sector to have moderately significant or less significant exposure to ML/TF risks, with very few CAs considering that the overall risk profile is significant or very significant (see Figure 41 for more details). Some CAs consider that there are inadequate levels of AML/CFT compliance among staff employed in this sector, when compared with other



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

sectors carrying out similar tasks. This has resulted in poor controls relating to the management of risks and the reporting of suspicious transactions, which is of particular concern to the CAs considering that CPs' business is generally based on processing large numbers of loans every day.

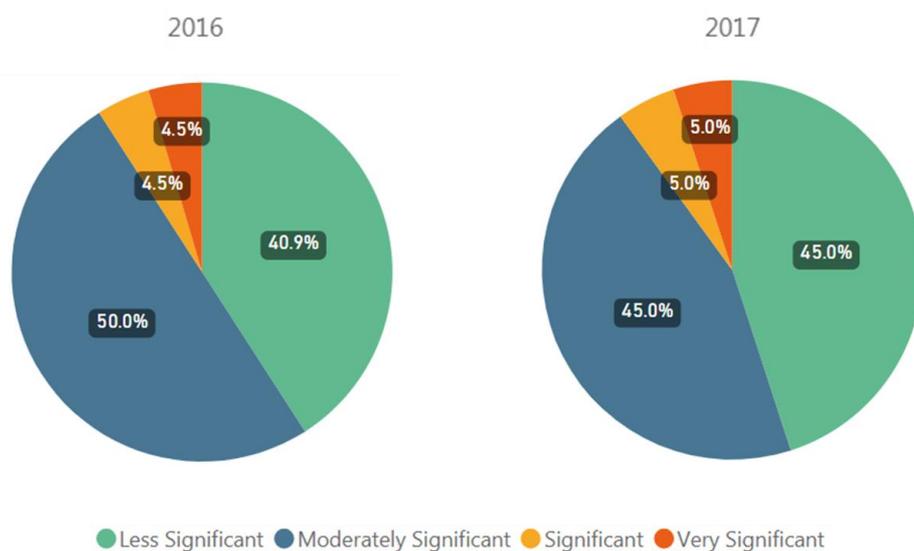


Figure 41: Overall ML/TF risk profile of the CPs' sector — 2016 versus 2017.

#### IV. EMERGING RISKS IN THE SECTOR

126. From the responses received, it appears that the sector's exposure to the risk of terrorist financing is considered as both a current and an emerging risk. CAs consider that the sector is particularly exposed to terrorist financing at a customer on-boarding stage, when customers may use false identities and false identification documents to obtain a credit and thereafter use these funds to finance terrorist attacks.

127. Similarly to other sectors, CAs are apprehensive about the ML/TF risks arising from potential loopholes in the legal/regulatory framework related to new technology-based products and services.

128. The withdrawal of the UK from the EU is also considered to present certain ML/TF risks in this sector. Some CAs envisage that a significant number of the UK-based CPs will want to



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

establish themselves in the EU after the withdrawal of the UK from the EU and that this would have an impact on the sector's inherent risk and its analysis by CAs.

## V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

129. As well as being aware of the diverse nature of this sector, CAs should also be able to identify the most serious ML/TF risks for each kind of operational segment in order to prioritise their supervisory action and focus their resources and activities on the most risky firms in this sector. Firms belonging to each of the segments should be aware of the ML/TF schemes that could affect their activity, and should put in place the most appropriate risk-mitigating measures and controls.

### 5.7 BUREAUX DE CHANGE

130. The ESAs received responses from 22 CAs responsible for the AML/CFT supervision of bureaux de change in respect of 2016 and from 19 CAs in respect of 2017. A significant majority of CAs offered input based on their supervisory perception of ML/TF risks rather than on a formal assessment. A few authorities were unable to provide data for all sets of questions, occasionally responding 'non-applicable/not available' (these have been excluded from the figures in this section to simplify the analysis).

## I. INHERENT RISK IN THE SECTOR

131. The assessments of CAs of the inherent risk for this sector are divergent and range from very significant to less significant (see Figure 42). The key risk-increasing factors include the prevalence of cash transactions, the anonymity of transactions and the proximity to border regions and itinerant communities (migrants, cross-border workers, asylum seekers and tourism). However, from the responses received, it appears that the concentration of firms presenting very significant or significant risk in the sector is very low and the majority of firms are considered as presenting less significant risk.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

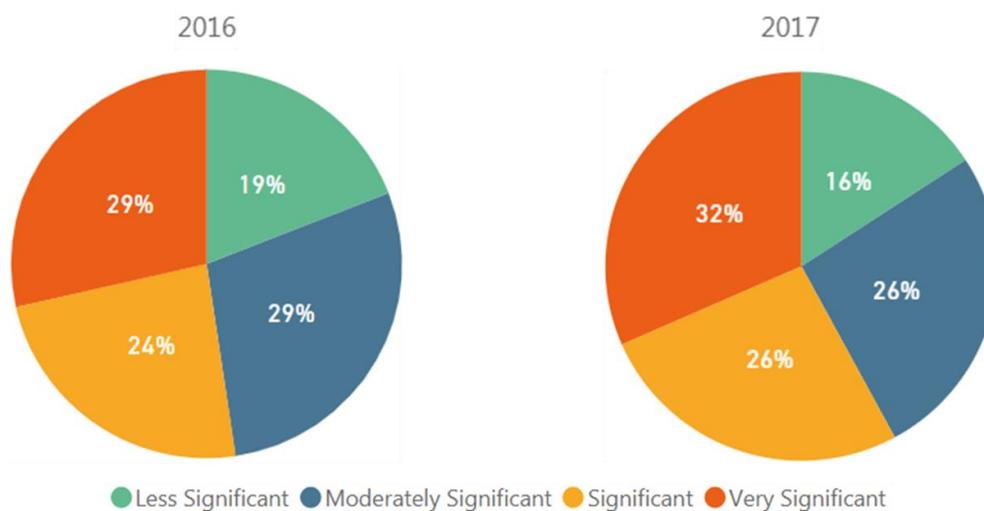


Figure 42: Inherent ML/TF risk profile of the bureau de change sector — 2016 versus 2017.

132. As regards the sector's exposure to ML/TF risks as a result of its cross-border activities, the majority of CAs consider the sector to present moderately significant or less significant risk. The CAs have highlighted the sector's increased exposure to geographical risk (i.e. high levels of activity near border regions and associated cash-intensive operations) as one of the risk-increasing factors in this area (see Figure 43 for more details).

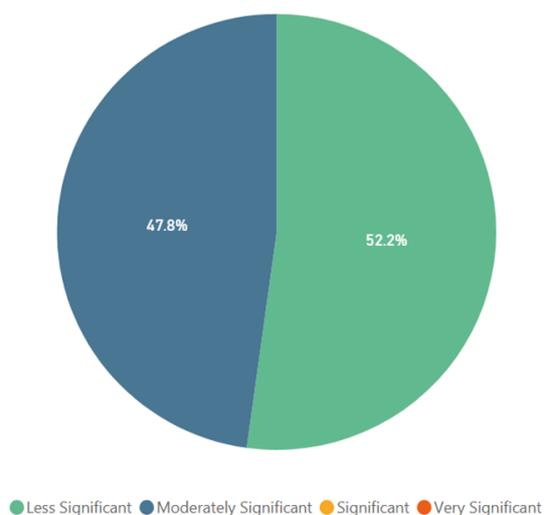


Figure 43: Bureau de change sector's exposure to ML/TF risks arising from cross-border activities.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

133. From the responses received, it is evident that CAs are particularly concerned about the adequacy and effectiveness of ongoing monitoring, STR and the assessment of customer ML/TF risks and have assessed these controls as poor or very poor (see Figure 44 for more details). This is of concern considering the nature of the business in this sector, which is largely based on cash transactions. However, the responses also show that a significant proportion of CAs have not carried out an assessment of controls in this sector.

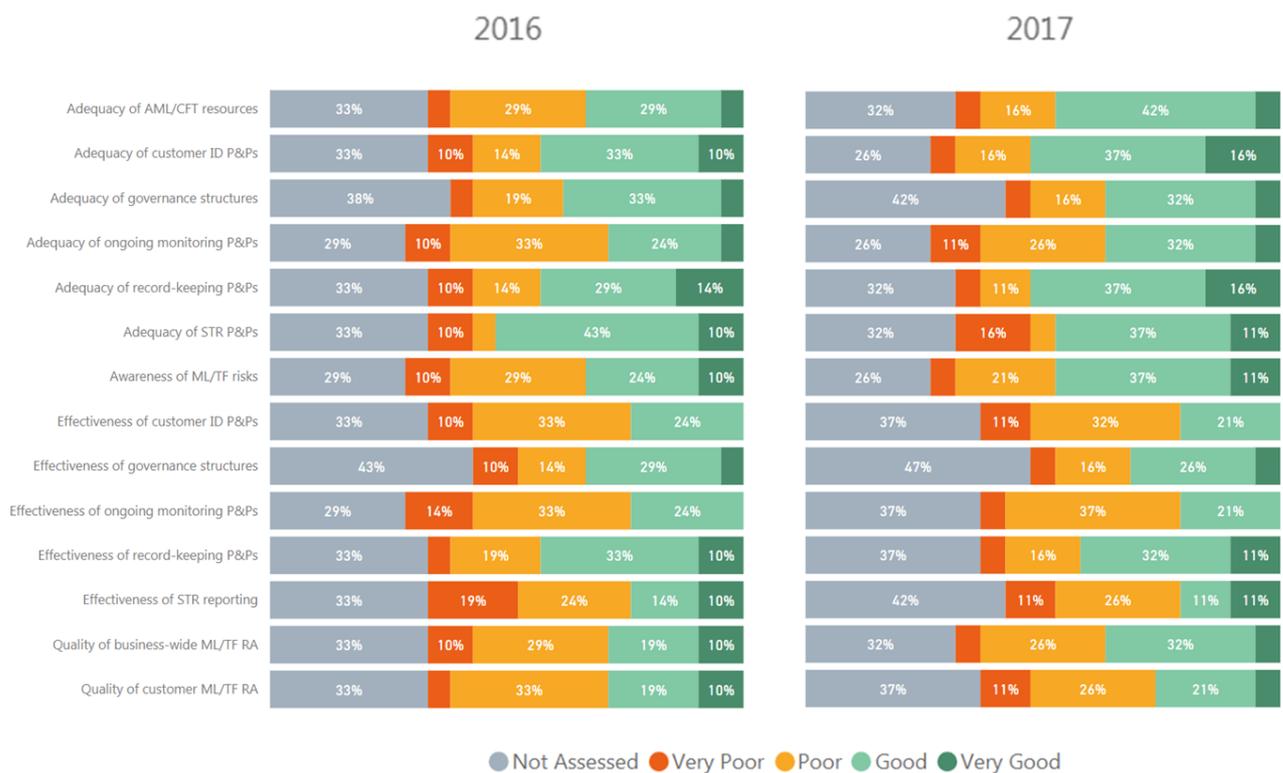


Figure 44: Quality of controls in the bureau de change sector — 2016 versus 2017.

134. The most common breaches identified in this sector coincide with the abovementioned assessment of controls, specifically pointing to poor controls related to customer identification and verification, STRs and deficiencies in the overall internal control framework, including AML/CFT policies and procedures (see Figure 45). The majority of breaches identified were minor or moderate (see Figure 46).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

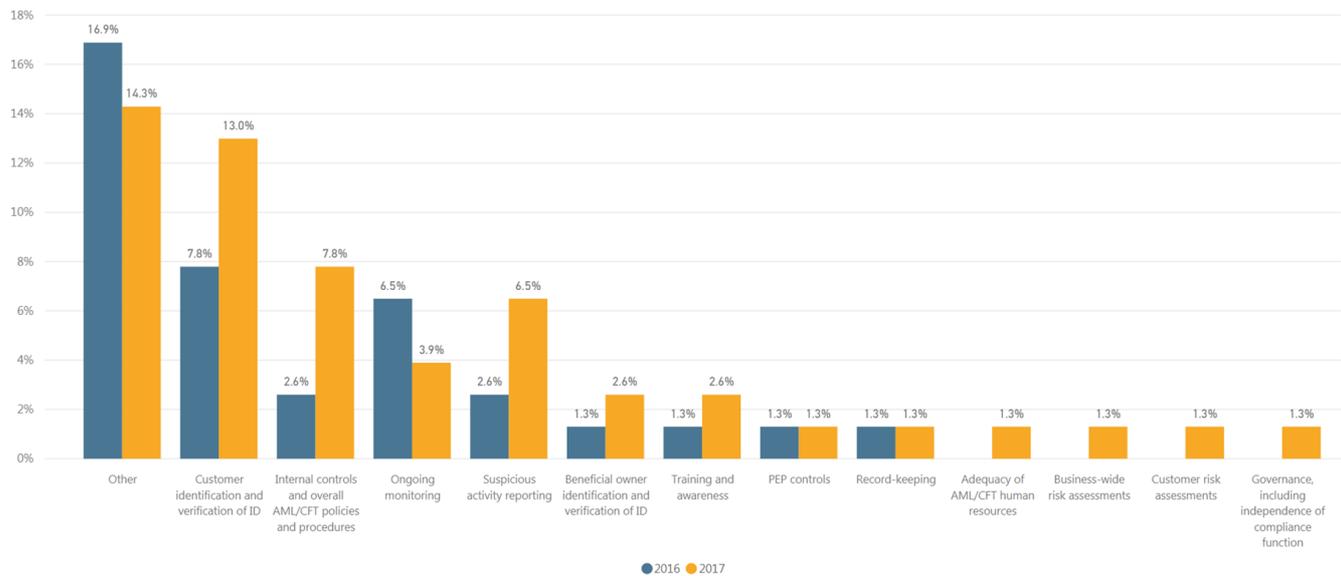


Figure 45: Most common types of breaches in the bureau de change sector — 2016 versus 2017.

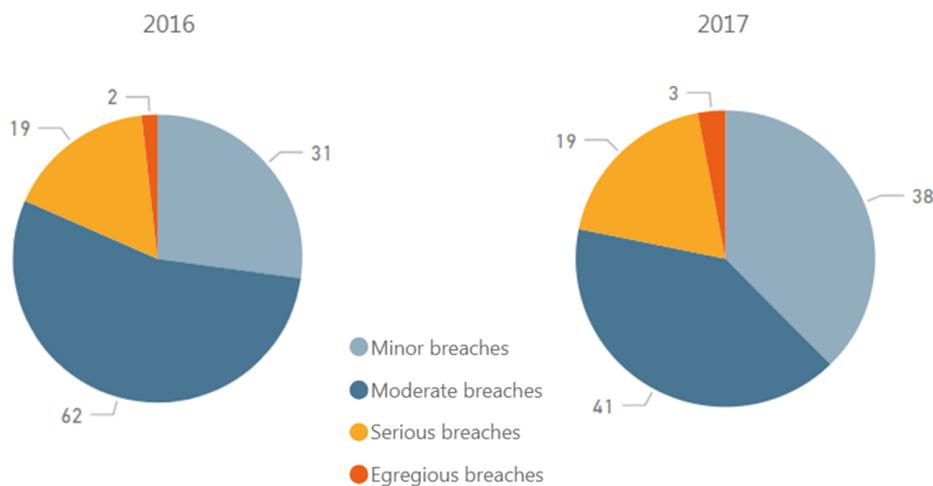


Figure 46: Number of breaches by their seriousness in the bureau de change sector — 2016 versus 2017.

### III. OVERALL RISK PROFILE OF THE SECTOR

135. The analysis of the sector's overall risk profile, which is rated as significant or very significant by a large proportion of CAs, suggests that the assessment of the quality of controls and mitigating measures still raises concerns for CAs (see Figure 47 for more details). In addition, many CAs stated that poor internal controls and the lack of awareness of the relevant regulatory



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

context, as well as poor STR practices, were ongoing risk factors, despite the controls implemented.

136. While the sector is considered to present a significant or very significant risk of ML/TF, the survey responses suggest that a large proportion of CAs have not carried out an assessment of controls in this sector. From the responses received, it is evident that supervisory activities focused on this sector have not been particularly intensive (see Figures 1 and 2). In the majority of cases, supervisory activities have been limited to offsite inspections, with some thematic inspections being carried out as a consequence of the concrete risks identified.

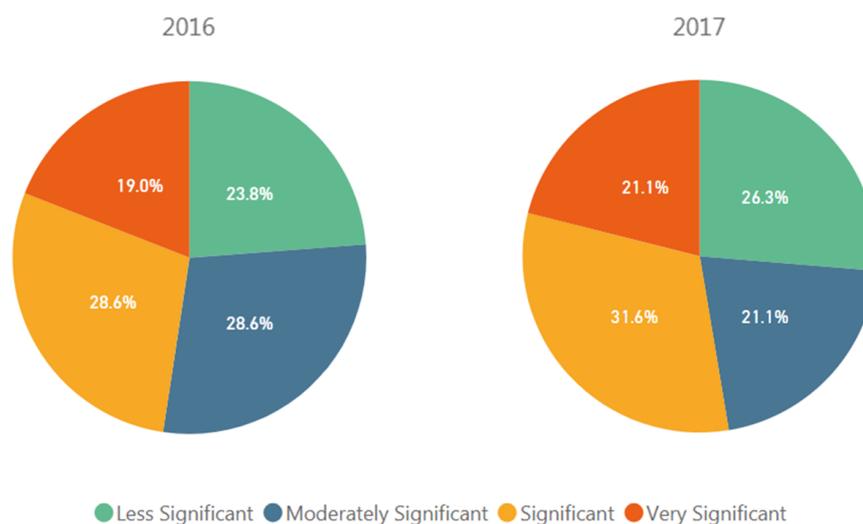


Figure 47: Overall ML/TF risk profile of the bureau de change sector — 2016 versus 2017.

#### IV. EMERGING RISKS IN THE SECTOR

137. The emerging risks identified in relation to this sector are generally linked to the risks and breaches identified. Firms' limited understanding of ML/TF risks, insufficiencies in firms' reporting practices and poor customer identification procedures are mentioned by the majority of CAs as both current and emerging risks. Overall, the nature of this sector's business, which is generally based on cash transactions, remains a source of concern for CAs.

138. The ESAs' contextual analysis of the responses received from CAs suggests that the development of new technologies may become an important mitigating force for this sector.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

The increase in online payments and the use of virtual currencies, while being viewed as an emerging risk in other sectors, may result in an enhancement of this sector by making it easier to identify ML/TF risks more effectively.

## V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

139. While it is evident from the responses received that there are different perceptions of the ML/TF risks associated with this sector across the EU, some CAs consider it to present significant or very significant risks. This raises concerns about low levels of supervisory activity in this sector. To implement the risk-based approach effectively, CAs are required to have a good understanding of the ML/TF risks present in all sectors, including those presenting a low and medium risk of ML/TF. Considering the low levels of supervisory activities and that a large proportion of CAs have not carried out an assessment of controls in this sector, the question arises of whether the CAs' understanding of the overall risk profile of this sector is sufficiently informed. Therefore, CAs that have not carried out any AML/CFT inspections of the sector should review their approach to AML/CFT supervision, with a view to obtaining sufficient information so that they can be reasonably satisfied that they understand the risks and controls put in place by firms in this sector.

140. In addition, a detailed analysis of controls in this sector suggests that actions must be taken by bureaux de change to improve the overall state of mitigating measures, in particular those related to the monitoring of transactions and STRs. Therefore, CAs may consider raising awareness of the existing ML/TF risks within the sector and communicating their expectations of what controls should be put in place to mitigate these risks to the sector. This could be achieved through increased outreach to firms in the sector, for example by publishing guidance on ML/TF risks or by providing additional guidance on the identification, assessment and submission of STRs.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## 5.8 INVESTMENT FIRMS

141. Alongside credit institutions, investment firms provide a range of services that give investors access to securities and derivatives markets. Such services include investment advice, portfolio management, executing orders on behalf of clients and dealing on own account.

142. The ESAs received responses from 33 CAs responsible for the AML/CFT supervision of investment firms in relation to 2016 and from 29 CAs in relation to 2017.

### I. INHERENT RISKS IN THE SECTOR

143. The majority of CAs rated the overall inherent ML/TF risk profile as moderately significant (see Figure 48). After a more granular examination of the sector's inherent risk rating associated with all four risk factor groups — products/services, customers, geographies and delivery channels — it is evident that only products/services have also been rated as moderately significant. Conversely, customers and geographies were rated as presenting very significant risk by some CAs. Delivery channels appeared to pose the lowest level of inherent risk overall.

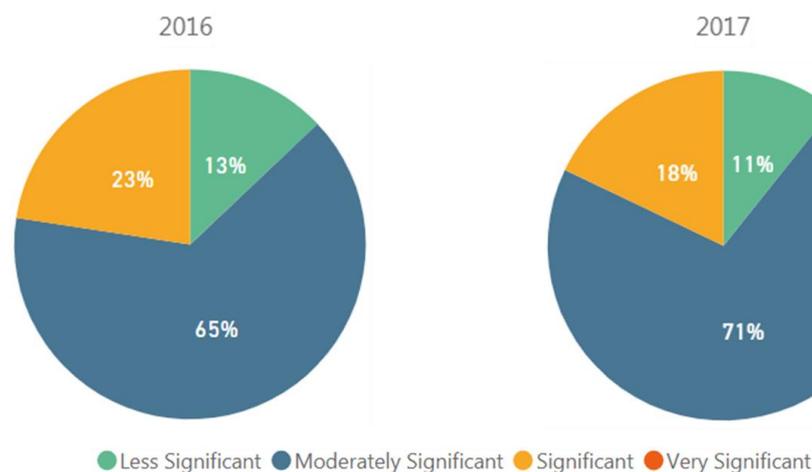


Figure 48: Inherent ML/TF risk profile of the investment firm sector — 2016 versus 2017.

144. A large proportion of CAs consider this sector to have a very significant exposure to ML/TF risks owing to its cross-border activities, as the firms in this sector often provide their products and services through passporting in other Member States (see Figure 49 for more details). For



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

firms with branches in different Member States, this often leads to additional challenges when they are trying to reconcile the AML/CFT standards of the home and host Member States.

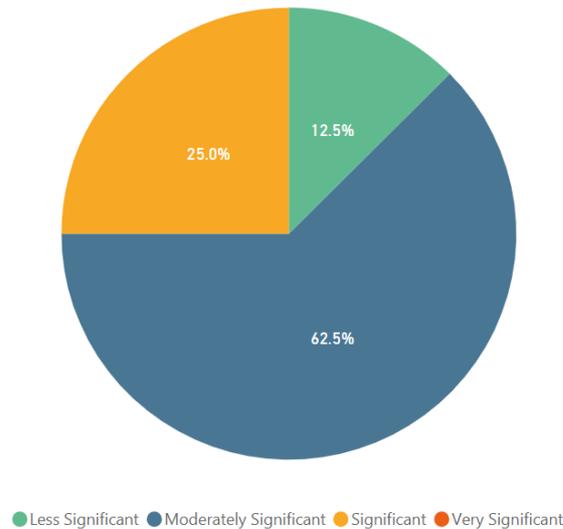


Figure 49: Investment firms' exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

145. From the responses received, it appears that CAs are particularly concerned about controls relating to STRs and ongoing monitoring, including transaction monitoring, and have rated these as very poor. This is of concern considering the nature of the business in this sector, which is based on large volumes of transactions being processed quickly. In contrast, the adequacy and effectiveness of record-keeping policies and procedures were the two controls that most CAs considered to be very good (see Figure 50 for more details).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

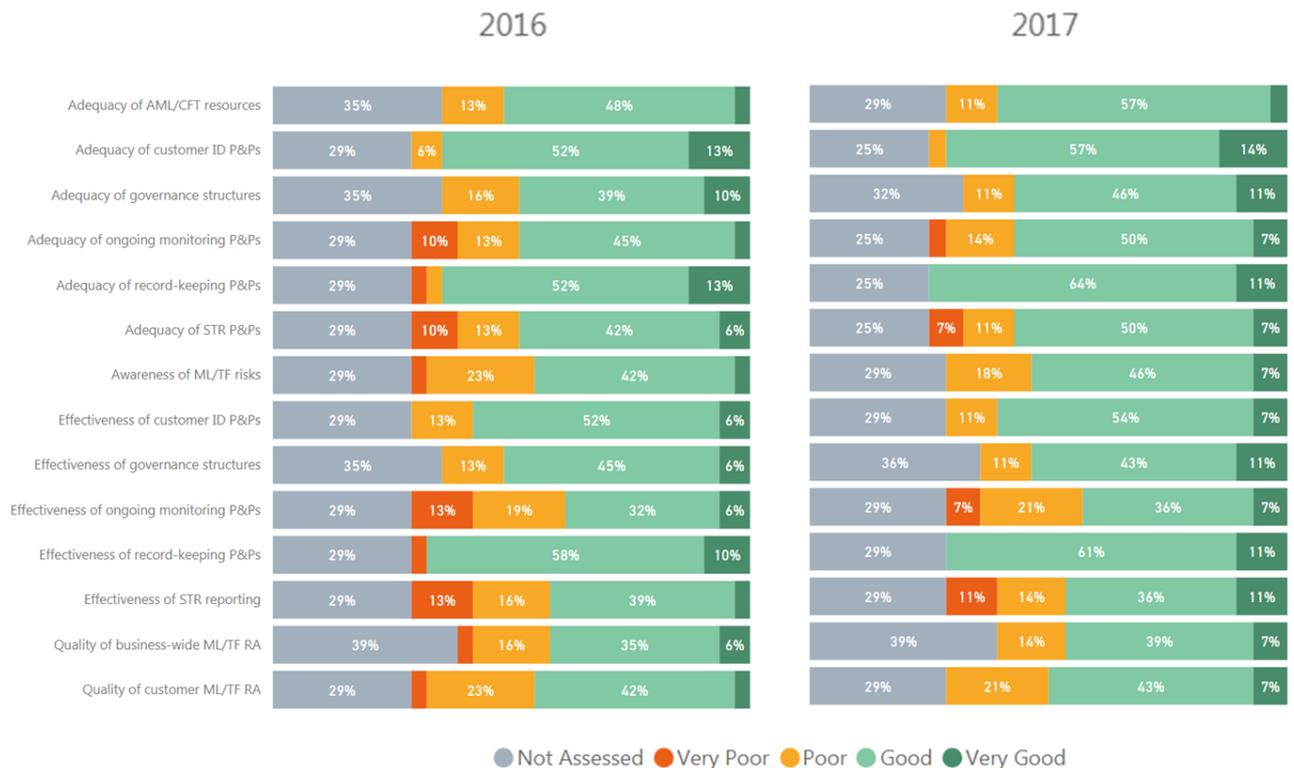


Figure 50: Quality of controls in the investment firm sector — 2016 versus 2017.

146. In terms of breaches, the four most common types of breaches identified in this sector relate to internal controls (including AML/CFT policies and procedures), controls related to customer identification and verification, ongoing monitoring and STRs (see Figure 51 for more details). However, it appears that the majority of breaches identified in 2017 were considered minor, with only very few breaches classified as serious or egregious, which is a change from 2016 when the majority of breaches were considered moderate (see Figure 52 for more details).

147. After examining the supervisory activities in this sector (see Figures 1 and 2), it appears that supervisors have mainly focused their activities on offsite inspections. This leads to the conclusion that, in a large number of cases, these breaches relate only to the adequacy of controls, as the effectiveness of controls can be fully assessed only through onsite inspections.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

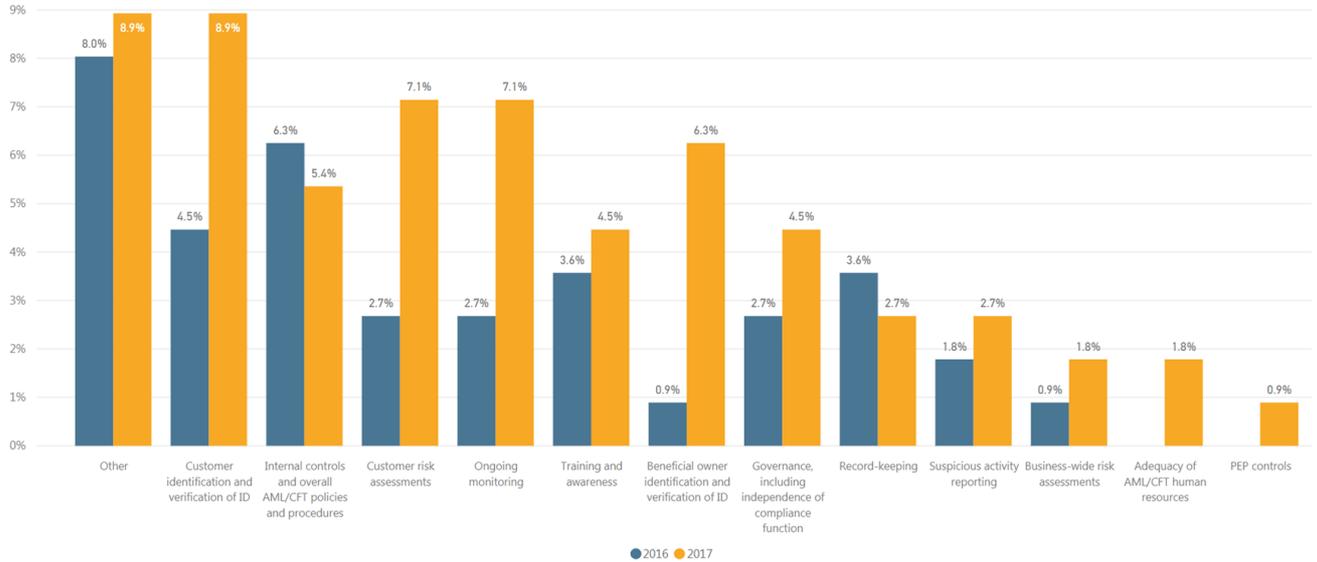


Figure 51: Most common types of breaches in the investment firm sector — 2016 versus 2017.

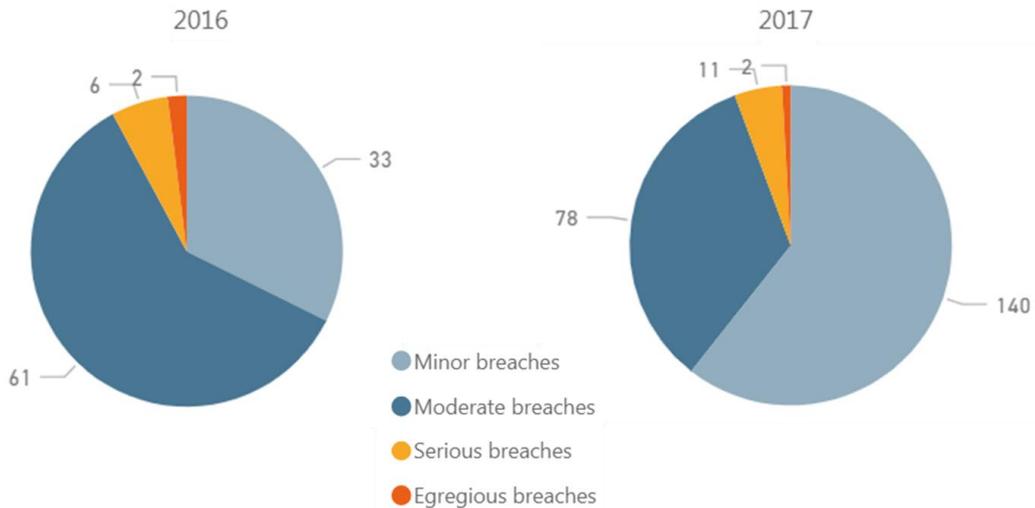


Figure 52: Number of breaches by their seriousness in the investment firms' sector — 2016 versus 2017.

### III. OVERALL RISK PROFILE OF THE SECTOR

148. The majority of CAs consider the overall risk of the sector to be moderately significant (see Figure 53 for more details). From the responses received, it appears that CAs attribute the sector's exposure to risks to its non-resident customer base, non-face-to-face transactions and concerns around links to tax havens.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

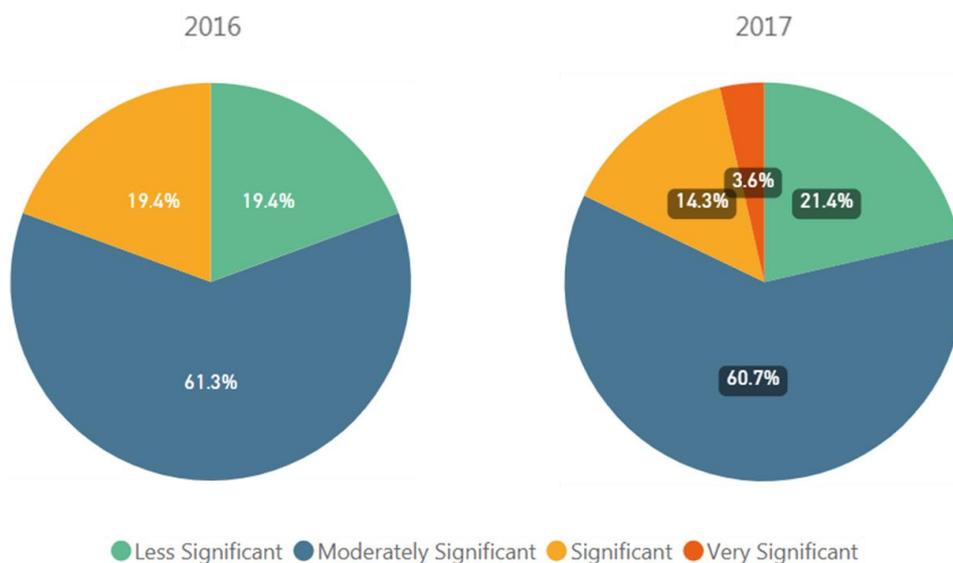


Figure 53: Overall ML/TF risk profile of the investment firm sector — 2016 versus 2017.

#### IV. EMERGING RISKS IN THE SECTOR

149. A number of CAs have raised concerns about innovation and new technologies used in this sector, with specific risks arising from peer-to-peer lending activities, high-frequency trading, initial coin offerings and virtual currencies.

#### V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

150. It is recommended that CAs consider whether or not:

- (i) their understanding of the overall ML/TF risk profile, which is based largely on offsite supervisory activities, is a true representation of the sector and, if necessary, they should review their approach to AML/CFT supervision of this sector with a view to obtaining sufficient information so that they can be reasonably satisfied that they understand the risks and controls put in place by firms in this sector;
- (ii) new or revised guidance is needed for the sector to emphasise the importance of these controls and to communicate supervisory expectation in this area.

151. In addition, CAs should continue to monitor broader technological and innovative developments in this sector and look to deepen their understanding of ML/TF risks and



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

opportunities that are more prevalent in this sector than in others. This will assist in identifying suitable controls to effectively manage emerging risks.

## 5.9 INVESTMENT FUNDS

152. A total of 30 CAs responsible for the supervision of investment funds' compliance with AML/CFT rules provided data for 2016 and 27 CAs provided data for 2017.

### I. INHERENT RISKS IN THE SECTOR

153. Investment funds are characterised by the often medium- to long-term nature of the investment, which can limit their attractiveness for ML/TF purposes. Therefore, most CAs assessed the overall level of inherent risk as moderately significant or less significant, with none of the CAs considering the sector to be exposed to a very significant risk of ML/TF (see Figure 54).

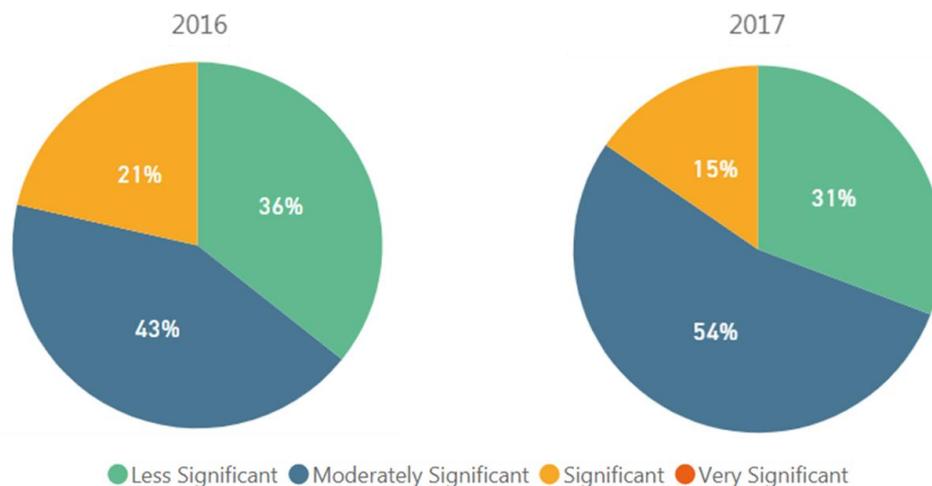


Figure 54: Inherent ML/TF risk profile of the investment fund sector — 2016 versus 2017.

154. A large proportion of CAs consider this sector to be exposed to a moderately significant ML/TF risk owing to its cross-border activities (see Figure 55 for more details), as this sector extensively uses passporting rights, which means that, while the fund might be registered in one Member State, it is often distributed across the EU. However, the exposure to ML/TF risk increases when funds are distributed outside the EU.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

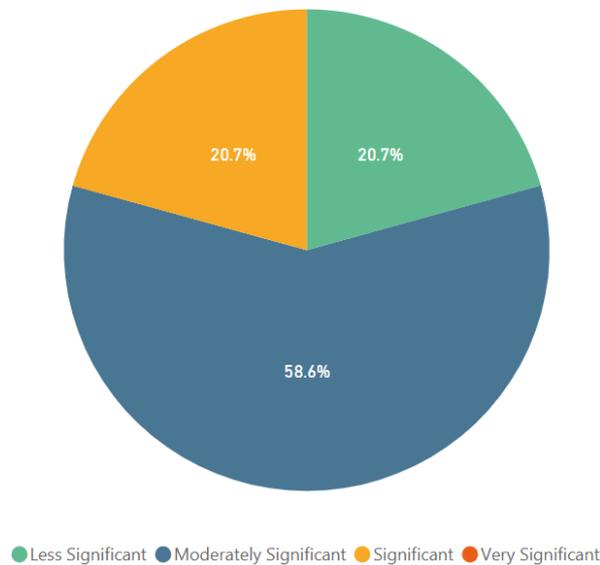


Figure 55: Investment funds' exposure to ML/TF risks arising from cross-border activities.

## II. QUALITY OF CONTROLS AND COMMON BREACHES IN THE SECTOR

155. Based on the responses from the CAs that had carried out assessments of controls within this sector, it appears that controls relating to ongoing monitoring and STRs are of particular concern. Many CAs rated these controls as poor or very poor. Overall, it appears that, while the policies and procedures that fund managers had put in place to comply with their AML/CFT obligations were often considered adequate, CAs found that these policies and procedures were not always applied effectively and that this affected fund managers' understanding of the risks associated with individual relationships and the risks to which they were exposed as a business. For example, around 60% of CAs considered that policies and procedures related to the identification and verification of customers and beneficial owners were good, but only 50% of CAs found them to be effective (see Figure 56 for more details). These findings are of concern in a sector in which the identity of the underlying investor is not always known by the fund manager. The provision and distribution of investment funds can legitimately involve multiple parties, which may affect how much the fund manager knows about the direct customers and underlying investors (when the investors are not direct customers). To mitigate the risks in situations where the investors are not customers, the application of robust CDD measures to customers in line with Chapter 9 of the ESAs' risk factors guidelines is particularly important.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

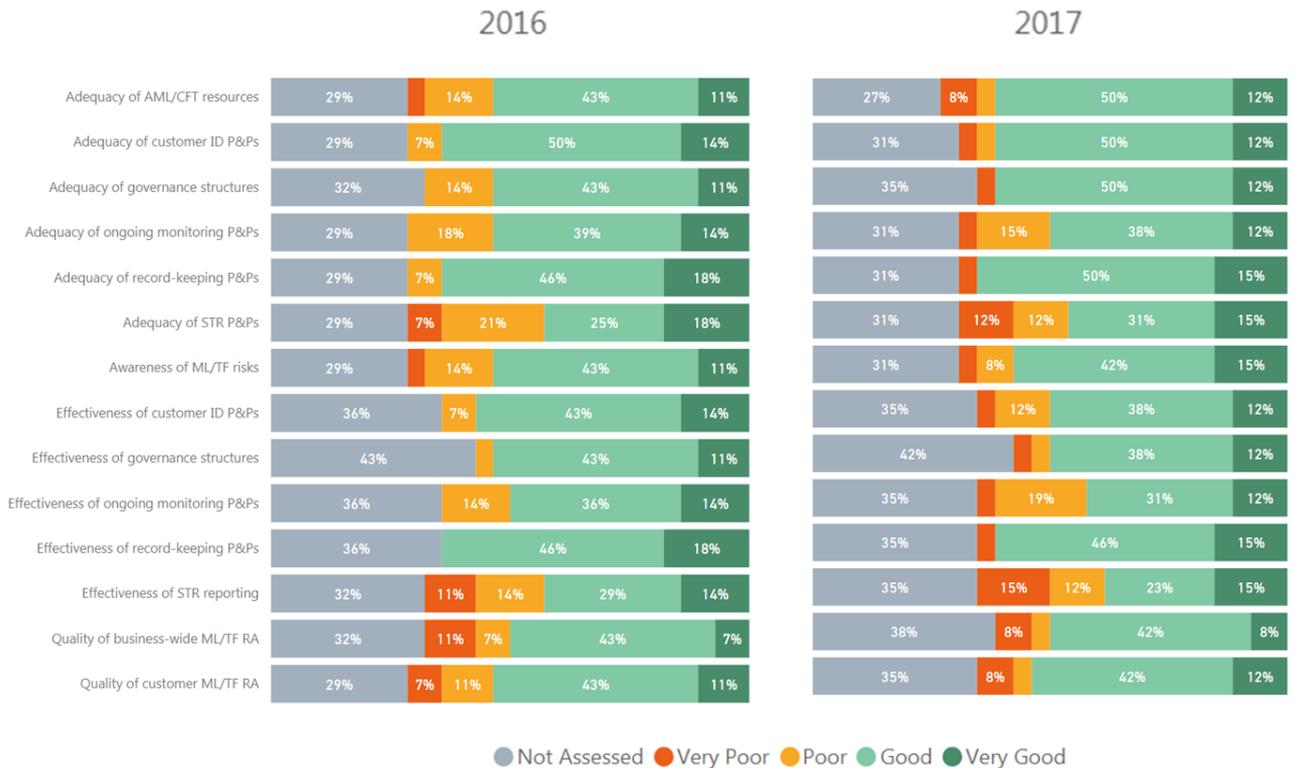


Figure 56: Quality of controls in the investment fund sector — 2016 versus 2017.

156. As the sector is considered to have a moderately significant or less significant inherent risk, the level of supervisory activity in this sector has been low, which is in line with the risk-based approach (see Figures 1 and 2). Therefore, only a small number of breaches have been identified and the majority of those have been classified as moderate or minor (see Figure 58). The breaches that were identified often related to the identification and verification of customers and beneficial owners, customer risk assessments and ongoing monitoring (see Figure 57 for more details).



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

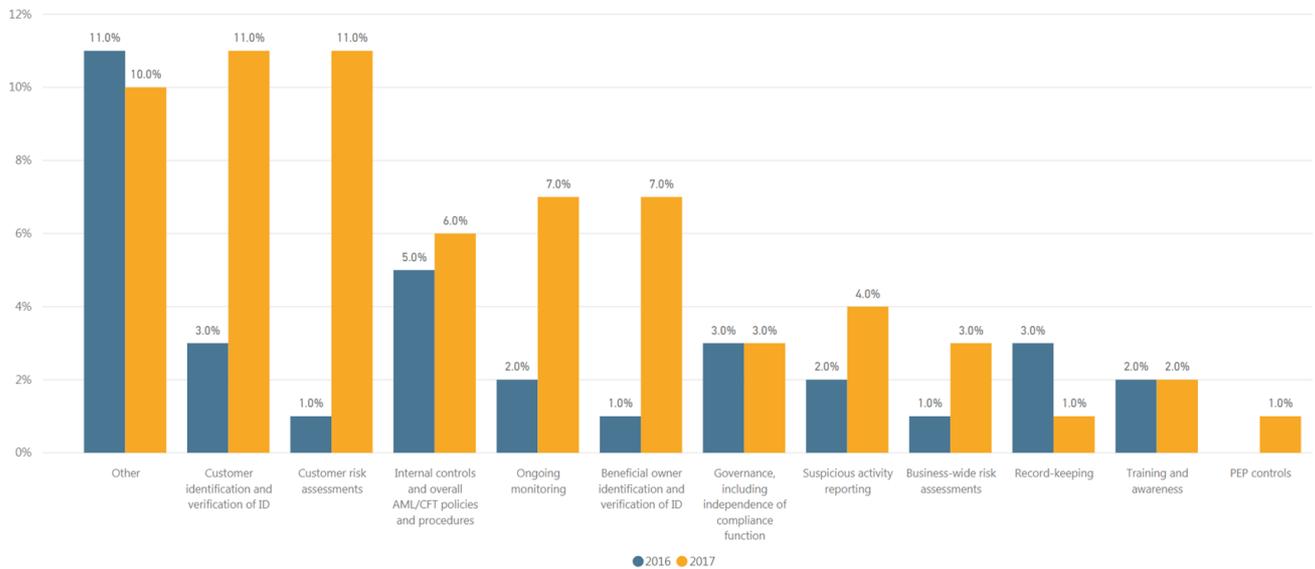


Figure 57: Most common types of breaches in the investment fund sector — 2016 versus 2017.

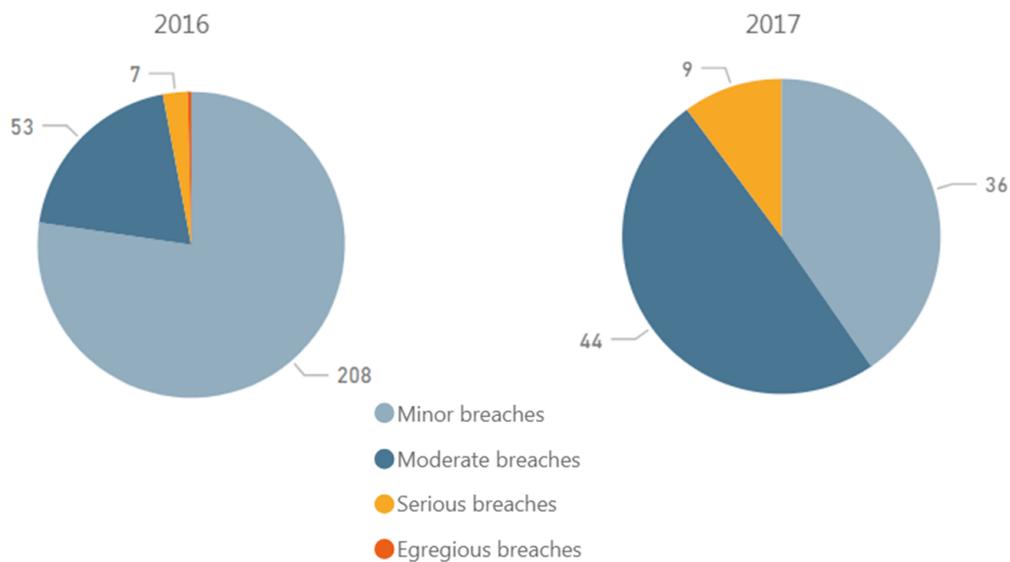


Figure 58: Number of breaches by their significance in the investment fund sector — 2016 versus 2017.

### III. OVERALL RISK PROFILE OF THE SECTOR

157. Most CAs rated the overall risk profile of the sector as moderately significant or less significant (see Figure 59), with only a small number of CAs viewing the risk associated with the sector as significant. However, contributing to this is the CAs' concerns about weaknesses in



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

controls relating to the identification of beneficial ownership owing to the use of intermediaries and the monitoring of transactions with high-risk countries, as well as the sector's different understandings of the CDD obligations as regards the fund or fund manager. As a result, fund managers may not be fully considering the ML/TF risk profile of their investors on an ongoing basis. Some CAs have also raised concerns about the adequacy of AML/CFT staff and their training and about inadequate IT support.

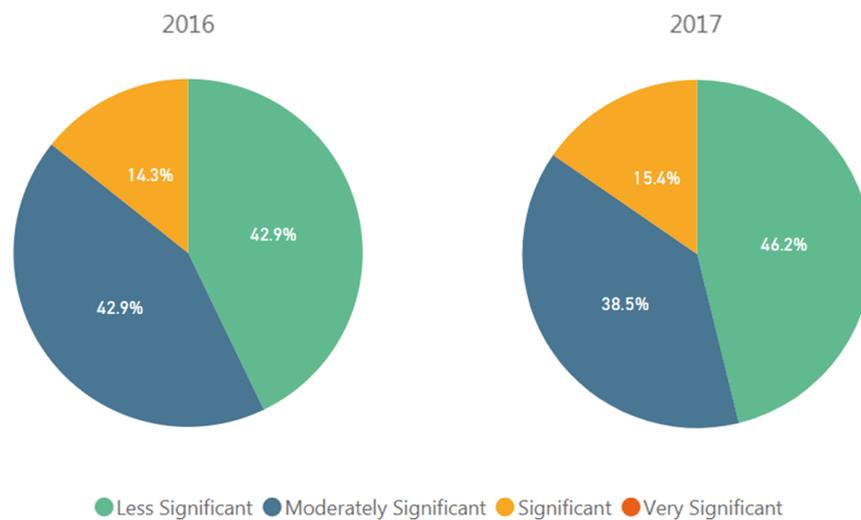


Figure 59: Overall ML/TF risk profile of the investment fund sector — 2016 versus 2017.

#### IV. EMERGING RISKS IN THE SECTOR

158. From the responses received, similar to other sectors, most CAs see future ML/TF vulnerabilities in this sector arising from technological developments (see subsection 4.2 for more details).

#### V. RECOMMENDATIONS FOR THE COMPETENT AUTHORITIES

159. While the sector might be considered to present relatively low ML/TF risks, there are particular areas in which the sector is vulnerable to ML/TF, which means that these areas may require enhanced supervisory attention. The failure of a significant number of firms across the EU to apply effective CDD measures is of particular concern in a sector in which intermediaries are used to distribute funds.



JOINT COMMITTEE OF THE EUROPEAN  
SUPERVISORY AUTHORITIES

160. Furthermore, previous policy work by the ESAs has highlighted that firms' and CAs' understanding of the CDD obligations in this sector differ owing to the variety of intermediary roles involved. It is important, therefore, that firms and CAs refer to Chapter 9 of the ESAs' Risk Factors Guidelines, which sets out a common understanding, on the part of EU CAs, of the measures that firms in this sector should take to meet their AML/CFT obligations.



## ANNEX I: DEFINITIONS

Term	Meaning
Firm	A credit institution or financial institution as defined in points (1) and (2) of Article 3 of AMLD4
Competent authority (CA)	The authority or authorities designated as the competent authorities for supervising and ensuring supervised entities' compliance with the requirements of AMLD4
Less significant risk	<p>For inherent risk:</p> <p>The combination of products, services, customers, geographies and delivery channels prevalent in the firm or in the sector means that the firm or the sector is very unlikely to be abused for ML/TF purposes</p> <p>For the risk profile:</p> <ul style="list-style-type: none"> <li>• the inherent risk is less significant and the risk profile remains unaffected by mitigation; or</li> <li>• the inherent risk is moderately significant or significant, but is effectively mitigated through AML/CFT systems and controls that are at least 'good'</li> </ul>
Moderately significant risk	<p>For inherent risk:</p> <p>The combination of products, services, customers, geographies and delivery channels prevalent in the firm or in the sector means that the firm or the sector is unlikely to be abused for ML/TF purposes</p> <p>For the risk profile:</p> <ul style="list-style-type: none"> <li>• the inherent risk is moderately significant and the risk profile remains unaffected by mitigation; or</li> <li>• the inherent risk is significant or very significant, but is effectively mitigated through AML/CFT systems and controls that are at least 'good'</li> </ul>
Significant risk	For inherent risk:



JOINT COMMITTEE OF THE EUROPEAN  
SUPERVISORY AUTHORITIES

	<p>The combination of products, services, customers, geographies and delivery channels prevalent in the firm or in the sector makes the firm or the sector likely to be abused for ML/TF purposes</p> <p>For the risk profile:</p> <ul style="list-style-type: none"> <li>• the inherent risk exposure is significant and the risk profile remains unaffected by mitigation; or</li> <li>• the inherent risk is very significant, but is effectively mitigated through AML/CFT systems and controls that are at least 'good'</li> </ul>
<p>Very significant risk</p>	<p>For inherent risk:</p> <p>The combination of products, services, customers, geographies and delivery channels prevalent in the firm or in the sector makes the firm or the sector very likely to be abused for ML/TF purposes</p> <p>For the risk profile:</p> <p>The inherent risk is very significant, but is not effectively mitigated owing to systemic AML/CFT system and control weaknesses in the firm or in the majority of firms in the sector</p>
<p>Scheduled onsite inspection</p>	<p>A comprehensive/full-scope onsite review of a firm's AML/CFT systems and controls that 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 AML/CFT compliance and a review of risk assessments and customer files</p>
<p>Ad hoc onsite inspection</p>	<p>An onsite review, whether comprehensive or focusing on a particular aspect of a firm'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), 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</p>
<p>Scheduled offsite inspection</p>	<p>A comprehensive/full-scope offsite review of a firm's AML/CFT systems and controls on the basis of written policies and procedures and risk assessments.</p>



JOINT COMMITTEE OF THE EUROPEAN  
SUPERVISORY AUTHORITIES

	Offsite inspections are scheduled in line with the risk-based approach and do not normally involve testing the implementation of these policies and procedures
Ad hoc offsite inspection	An offsite review, whether comprehensive or focusing on a particular aspect of a firm'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), 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
Thematic inspection	Onsite or offsite reviews of a number of firms, often from the same sector, that focus on one specific aspect or very few aspects of these firms' AML/CFT systems and controls, such as transaction monitoring or the treatment of politically exposed persons. Thematic reviews often serve to help supervisors gain a better understanding of the way that specific ML/TF risks are managed by a sector or by particular types of firms
AML/CFT returns	Regular or ad hoc requests to firms for quantitative data relating to key ML/TF risk indicators  AML/CFT returns are different from offsite inspections in that they 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	The action that supervisors take to address shortcomings or breaches of firms' AML/CFT obligations. Supervisory action can range from a letter setting out recommendations to the imposition of pecuniary sanctions or the withdrawal of permissions
Risk	The likelihood and impact of money laundering or terrorist financing taking place  Inherent risk refers to the level of ML/TF risk before mitigation and a firm's or a sector's risk profile refers to the residual level of ML/TF risk that remains after inherent risks have been mitigated
Investment funds/ asset managers	<ul style="list-style-type: none"> <li>'Alternative investment fund managers' is used as defined under Article 4(1)(b) of Directive 2011/61/EU</li> </ul>



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

	<ul style="list-style-type: none"> <li>• ‘Management companies’ is used as defined under Article 2(1)(b) of Directive 2009/65/EC</li> <li>• ‘Alternative investment funds’ is used as defined under Article 4(1)(a) of Directive 2011/61/EU;</li> <li>• ‘Undertakings for collective investment in transferable securities’ is used as defined under Article 1(2) of Directive 2009/65/EC, marketing its units or shares</li> </ul>
FinTech	‘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’ (Financial Stability Board)
RegTech	‘The use of new technologies to solve regulatory and compliance requirements more effectively and efficiently’ (Institute of International Finance)