EBA/CP/2025/20

7 August 2025

Consultation Paper on

Draft revised Guidelines

on internal governance under Directive 2013/36/EU

Contents

Responding to this consultation

The EBA invites comments on the tracked amendments to these Guidelines.

Comments are most helpful if they:

- indicate the specific article to which the comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternatives the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 07.11.2025. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 f the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the EBA website.

Executive summary

For several years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct institutions' weak or superficial internal governance practices, as identified during the financial crisis and supervisory practices. Recently, there has been a greater focus on conduct-related shortcomings, including compliance with the framework to prevent money laundering and terrorist financing and regarding activities in offshore financial centres. Increased innovation including digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. In this regard, it is necessary to further reinforce institutions' sound governance arrangements.

Sound internal governance arrangements are fundamental if institutions, individually and the banking system they form, are to operate well. Directive 2013/36/EU, as amended by Directive (EU)2024/1619 and Directive 2019/878/EU, reinforces the governance requirements for institutions and in particular, stresses the responsibility of the management body for sound governance arrangements; the importance of a strong supervisory function that challenges management decision-making; the role of key function holders and the need to establish and implement a sound risk strategy, risk appetite and risk management framework.

To further harmonise institutions' internal governance arrangements, processes and mechanisms within the EU in line with the requirements of Directive 2013/36/EU, the European Banking Authority (EBA) is mandated by Article 74(3) of Directive 2013/36/EU to develop guidelines. The guidelines apply to all institutions regardless of their governance structures (unitary board, dual board or other structure), without advocating or preferring any specific structure.

The guidelines complete the various governance provisions in Directive 2013/36/EU, taking into account the principle of proportionality, by specifying the tasks, responsibilities and organisation of the management body, and the organisation of institutions, including the need to create transparent structures that allow for supervision of all their activities; the guidelines aim at ensuring the sound management of risks across all three lines of defence and, in particular, set out detailed elements for the second line of defence (the risk management and compliance function) and the third line of defence (the internal audit function).

The EBA Guidelines have been amended to reflect the changes introduced by Directive (EU) 2024/1619[1] and to take into account the results of the EBA benchmarking report of diversity practices and gender neutral remuneration policies. As part of robust governance arrangements and in light of Article 151 and 153 TFEU[2], the Guidelines reinforce equality among genders, but also diversity and inclusion. The guidelines take also into account the lessons learnt from supervisory practices. The public consultation is limited to the changes introduced to the guidelines.

[1] Directive (EU) 2024/1619 of the European Parliament and of the Council of 31 May 2024 amending Directive 2013/36/EU as regards supervisory powers, sanctions, third-country branches, and environmental, social and governance risks

[2] Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390

Background and rationale

1. Trust in the reliability of the financial system is crucial for its proper functioning and a prerequisite if it is to contribute to the economy as a whole. Consequently, effective internal governance arrangements are fundamental if institutions, individually and the banking system they form, are to operate well.

2. For several years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct institutions' weak or superficial internal governance practices, as identified during the financial crisis and from supervisory reviews . These faulty practices, while not a direct trigger for the financial crisis, were closely associated with it and were questionable. In addition, recently, there has been a greater focus on conduct-related shortcomings and activities in offshore financial centres, as well as a greater focus on the role of institutions to contribute to address challenges related to environmental, social and governance (ESG) factors. Increased innovation including digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions.

3. In some cases, at the time of the financial crisis the absence of effective checks and balances within institutions resulted in a lack of effective oversight of management decision-making, which led to short-term oriented and excessively risky management strategies. Weak oversight by the management body in its supervisory function has been identified as a contributing factor. The management body, both in its management function and, in particular, in its supervisory function, might not have understood the complexity of the business and the risks involved, consequently failing to identify and constrain excessive risk-taking in an effective manner.

4. Internal governance frameworks, including internal control mechanisms and risk management, were often not sufficiently integrated within institutions or groups. There was a lack of a uniform methodology and terminology, so that a holistic view of all risks did not exist. Internal control functions often lacked appropriate resources, status and/or expertise.

5. Conversely, sound internal governance practices helped some institutions to manage the financial crisis significantly better than others. These practices included the setting of an appropriate risk strategy and appropriate risk appetite levels, a holistic risk management framework and effective reporting lines to the management body.

6. Against this background, there is a clear need to address and reinforce the potentially detrimental effects of poorly designed internal governance arrangements on the sound management of risk, to ensure effective oversight by the management body, in particular in its supervisory function, to promote a sound risk culture and a strong internal control

framework and at all levels of institutions and to enable competent authorities to supervise and monitor the adequacy of internal governance arrangements.

7. The EBA Guidelines have been amended to reflect the changes introduced by Directive (EU) 2024/1619 and to take into account the results of the EBA benchmarking report of diversity practices and gender neutral remuneration policies. As part of robust governance arrangements and in light of Articles 151 and 153 of TFEU , the Guidelines reinforce equality among genders, diversity and inclusion, which also should support the creation of a gender balanced pool of candidates for positions within the management body.

8. The Guidelines are also amended to specify further the requirements introduced by Article 48(g) of Directive (EU) 2024/1619 on third country branches'sound internal governance arrangements taking into account third country branches specificities.

Legal basis

9. The guidelines apply in the same way to institutions as to investment firms that are subject to Title VII of Directive 2013/36/EU [3] in application of Article 1(2) and (5) of Regulation 2019/2033/EU.

10. To further harmonise institutions' internal governance arrangements, processes and mechanisms within the EU, the EBA is mandated in accordance with Article 74(3) of Directive 2013/36/EU to develop guidelines in this area. EBA is also mandated under Article 48g(9) of Directive 2013/36/EU to develop guidelines on third-country branches' internal governance arrangements, processes and mechanisms referred to in Article 74 (1) of Directive 2013/36/EU, taking into account Article 74(2), and on the application to third-country branches of Article 75 and Article 76(5) and (6) of Directive 2013/36/EU .

11. Article 74(1) of Directive 2013/36/EU requires institutions to have robust governance arrangements, which include: (a) a clear organisational structure with well-defined, transparent and consistent lines of responsibility; (b) effective processes to identify, manage, monitor and report the risks they are or might be exposed to, including ESG risks in the short, medium and long term of at least 10 years (c) adequate internal control mechanisms, including sound administration and accounting procedures; (d) network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554; (e) gender neutral remuneration policies and practices that are consistent with and promote sound and effective risk management, including by taking into account the institutions' risk appetite in terms of ESG risks.'

12. Article 76 of Directive 2013/36/EU sets out requirements for the involvement of the management body in risk management and for the management of risks resulting from

[3] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC

current and future impacts of ESG factors including through specific plans, quantifiable targets and processes to address them[4], the setting up of a risk committee for significant institutions, and the tasks and organisation of the internal control functions as defined under Article 3(1)(9b) of Directive 2013/36/EU. In addition, this Article establishes 'that the heads of the internal control functions should be independent senior managers with distinct responsibility for the internal control functions', the notion of senior management being defined by Directive 2013/36/EU. To reflect the wording of the directive, the revised guidelines refer, regarding the second line of defence, to the 'risk management function' and to the 'compliance function' and regarding the third line of defence, to the 'internal audit function'. However, it should be remembered that business lines or units, as the first line of defence, have a material role in ensuring robust risk management and compliance within an institution.

13. Article 88 of Directive 2013/36/EU sets out the responsibilities of the management body regarding governance arrangements, including the segregation of duties in the organisation and the prevention of conflicts of interest. Institutions should also draw up, maintain and update individual statements setting out the roles and duties of all members of the management body in its management function, of senior management and of key function holders and a mapping of duties. Moreover, the directive sets out that Member States shall ensure that data on loans to members of the management body and their related parties are properly documented and made available to competent authorities upon request. Significant institutions are obliged under Paragraph 2 of this article to set up a nomination committee, unless under national law, the management body does not have any competence in the process of selection and appointment of any of its members.

14. Under Article 109(1) of Directive 2013/36/EU, competent authorities must require institutions to meet the obligations set out in Articles 74 to 96 of that directive on an individual basis, unless competent authorities make use of the derogations as defined in Article 7 of Regulation (EU) No 575/2013 or waivers for institutions permanently affiliated to a central body in compliance with Article 21 of Directive 2013/36/EU.

15. Under Article 109 (2) of Directive 2013/36/EU these guidelines apply on a sub-consolidated or consolidated basis. For this purpose, parent undertakings and subsidiaries subject to Directive 2013/36/EU must ensure that internal governance arrangements, processes and mechanisms in their subsidiaries are consistent, well integrated and that the governance arrangements on a consolidated basis are robust. In particular, it should be ensured that parent undertakings and subsidiaries subject to this directive implement such arrangements, processes and mechanisms in their subsidiaries not subject to this directive, including those established in third countries, including offshore financial centres. These arrangements, processes and mechanisms must also be consistent and well integrated and those subsidiaries not subject to this directive must also be able to produce any data and information relevant to the purpose of supervision. As set out in Article 109(2) of Directive 2013/36/EU, subsidiary

[4] Article 76 further categorizes future impacts as short-, medium- and long-term impacts, and also requires that Member States shall ensure a proportionate application of these requirements.

undertakings that are not themselves subject to this directive shall comply with their sector-specific requirements on an individual basis.

16. In accordance with Article 109(3) of Directive 2013/36/EU, the requirement under Article 109(2) of this directive to ensure the application of Articles 74 to 96 of the directive also in subsidiaries not themselves subject to this directive does not apply only, if the EU parent institution can demonstrate that the application is unlawful under the law of the third country where the subsidiary is established. With regard to the application of the remuneration requirements laid down in Articles 92, 94 and 95 of Directive 2013/36/EU, Article 109(4) of that directive foresees that those provisions should not apply on a consolidated basis to subsidiaries that are not themselves subject to this directive under certain specific conditions[5].

17. Under Article 123(2) of Directive 2013/36/EU, competent authorities must require institutions to have in place adequate risk management processes and internal control mechanisms, including sound reporting and accounting procedures in order to identify, measure, monitor and control transactions with their parent mixed-activity holding company and its subsidiaries appropriately.

18. Where Article 48(g) of Directive 2013/36/EU sets out requirements that are also applicable to institutions within the Member State where the branch is located, those requirements should be applicable, in principle, in the same manner. Regarding internal governance arrangements it needs to be taken into account that the branch does not have a management body, but should have at least two persons who are responsible for effectively directing the business. In particular, in line with Article 48g(1) of Directive 2013/36/EU, these "…persons shall be of sufficiently good repute and possess sufficient knowledge, skills and experience and commit sufficient time to the performance of their duties"[6]. Third country-branches should have in place robust governance frameworks, including a clear organisational structure and well-defined, transparent and consistent lines of responsibility and internal control fonctions independent from the operational functions. Third-country branches should establish sound remuneration policies, they shall have adequate resources to monitor and manage their third party risks, and manage their counterparty credit risk when they engage in back-to-back or intragroup operations.

19. Third-country branches and subsidiaries cannot be empty shells that do not have within the EU the sufficient substance to be authorised.

20. These guidelines should be read in conjunction with other relevant EBA guidelines, including the EBA guidelines on the sound management of third-party risk , the joint EBA and European Securities and Markets Authority (ESMA) guidelines on the assessment of the suitability of

[5] See EBA guidelines on sound remuneration policies

[6] See Joint EBA and ESMA Guidelines on the assessment of the suitability of members of the management body and key function holders https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/joint-esma-and-eba-guidelines

members of the management body and key function holders, the EBA guidelines on sound remuneration policies, the EBA guidelines on the management of ESG risks and the EBA guidelines on the supervisory review and evaluation process (SREP).

Rationale and objective of the guidelines

21. Internal governance includes all standards and principles concerned with setting an institution's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined, clearly allocated and how duties are mapped; how reporting lines are set up and what information they convey; and how the internal control framework is organised and implemented, including accounting procedures and remuneration policies. Internal governance also encompasses sound information and communication technology (ICT), third-party risk management including outsourcing arrangements and business continuity management.

22. Combating money laundering and terrorist financing is essential for maintaining stability and integrity in the financial system. Uncovering involvement of an institution in money laundering and terrorist financing might have an impact on its viability and the trust in the financial system. Together with the authorities and bodies (e.g. AML supervisors and financial intelligence units) responsible for ensuring compliance with anti-money laundering rules under Directive (EU) 2015/849, competent authorities have an important role to play in identifying and tackling weaknesses. In this context, the guidelines clarify in line with Directive 2013/36/EU that identifying, managing and mitigating money laundering and financing of terrorism risk is part of sound internal governance arrangements and credit institutions' risk management framework.

23. In the same way and in accordance with the amendments of May 2024 to Directive 2013/36/EU and Regulation (EU) No 575/2013, institutions should take into account environmental, social and governance (ESG) risks within their risk management framework, in line with the requirements set out by the EBA guidelines on the management of ESG risks.

24. Directive 2013/36/EU sets out requirements aimed at remedying weaknesses that were identified during the financial crisis regarding internal governance arrangements and in particular the sound management and oversight of risks. Identified weaknesses included in particular a lack of effective oversight by the management body, in particular in its supervisory function, limited accessibility of the supervisory function and shortcomings regarding the authority, stature and resources of the risk management function.

25. In addition, it is also necessary to take into account the relevant developments since the publication of the revised EBA guidelines on internal governance in 2021, such as the publication of the EBA guidelines on the management of ESG Risks[7], and the entry into force

[7] https://www.eba.europa.eu/activities/single-rulebook/sustainable-finance/guidelines-management-esg-risks

of the digital operational resilience framework under Directive (EU) 2022/2554[8] which provides organisational and governance requirements applicable to the management of ICT risk and requires the ICT risk management function to be organised according to the three lines of defense model taking into account the application of the principle of proportionality. The requirements introduced by Regulation (EU) 2024/1689[9] on providing artificial intelligence systems and the risks of fundamental rights violation and discrimination have been taken into account. In line with their previous revision, the guidelines align the terminology used regarding risk appetite and risk tolerance with the EBA guidelines on common procedures and methodologies for the SREP and also with the revised corporate governance principles for banks published by the Basel Committee on Banking Supervision (BCBS)[10]; they use the term 'risk appetite' to refer to the aggregate level of risk and the types of risk an institution is willing to assume, while 'risk capacity' is the maximum amount of risk an institution is able to assume.

26. The guidelines are intended to apply to all existing board structures without interfering with the general allocation of competences in accordance with national company law or advocating any particular structure. Accordingly, they should be applied irrespective of the board structure used (a unitary and/or a dual board structure and/or another structure) across Member States.. The management body, as defined in Points (7) and (8) of Article 3(1)of Directive 2013/36/EU, should be understood as having management (executive) and supervisory (non-executive) functions.

27. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law.

28. In Member States where the management body appoints persons that effectively direct the business of the institution, those persons belong, in accordance the Article 3(1)(8a) of Directive 2013/36/EU, to the management function of the management body.

29. The management body is empowered to set the institution's strategy, objectives and overall direction, and oversees and monitors management decision-making. The management body in its management function directs the institution. Senior management is accountable to the management body for the day-to-day running of the institution. The management body in its supervisory function oversees and challenges the management function and provides appropriate advice. The oversight roles include reviewing the performance of the

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2556

[9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (OJ L, 2024/1689, 12.7.2024)

[10] The BCBS principles can be found at http://www.bis.org/bcbs/publ/d328.htm.

management function and the achievement of objectives, challenging the strategy, and - monitoring and scrutinising the systems that ensure the integrity of financial information as well as the soundness and effectiveness of risk management and internal controls.

30. Taking into consideration all existing governance structures provided for by national laws, competent authorities should ensure the effective and consistent application of the guidelines in their jurisdictions in accordance with the rationale and objectives of the guidelines themselves. For this purpose, competent authorities may clarify the governing bodies and functions to which the tasks and responsibilities set forth in the guidelines pertain, when this is appropriate to ensure the proper application of the guidelines in accordance with the governance structures provided for under national company law.

31. Independent directors within the supervisory function of the management body helps to ensure that the interests of all internal and external stakeholders are considered and that independent judgement is exercised where there is an actual or potential conflict of interest[11].

32. With regard to the composition of committees and, in particular, with regard to independent members, the guidelines are in line with the BCBS principles on corporate governance, which set out guidance for the largest institutions. To take into account the principle of proportionality, simpler elements have been introduced for smaller institutions.

33. The guidelines are consistent with the 'three lines of defence' model in identifying the functions within institutions responsible for addressing and managing risks.

34. The business lines, as part of the first line of defence, take risks and are responsible for their operational management directly and on a permanent basis. For that purpose, business lines should have appropriate processes and controls in place that aim to ensure that risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the institution's risk appetite and that the business activities are in compliance with external and internal requirements.

35. Not only business lines, but also other functions or units, e.g. HR, legal or ICT, are responsible for managing their risks and having appropriate controls in place. Other functions or units are mainly exposed to operational and reputational risks that must be considered by the compliance function and risk management function when forming an enterprise-wide holistic view on all risks. All other functions or units should also be subject to the monitoring and oversight by the risk management and compliance functions on a risk-based approach.

36. The risk management function and compliance function form the second line of defence. Institutions may set up additional specific functions within the second line of defence (e.g. control function to manage and oversee ICT risk as referred to in article 6(4) of Regulation (EU) 2022/2554 or AML compliance function). The risk management function facilitates the

[11] In this regard, the guidelines are based on the Commission Recommendation of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board.

implementation of a sound risk management framework throughout the institution and has responsibility for further identifying, monitoring, analysing, measuring, managing and reporting risks and forming a holistic view on all risks on an individual and consolidated basis. It challenges and assists in the implementation of risk management measures by the business lines in order to ensure that the process and controls in place at the first line of defence are properly designed and effective. The compliance function monitors compliance with legal requirements and internal policies, provides advice on compliance to the management body and other relevant staff, and establishes policies and processes to manage legal risk stemming from non-compliance events and to ensure compliance. Both functions may intervene to ensure the modification of internal control and risk management systems within the first line of defence where necessary.

37. The internal audit function, as the third line of defence, conducts risk-based and general audits and reviews the internal governance arrangements, processes and mechanisms to ascertain that they are sound and effective, implemented and consistently applied. The internal audit function is also in charge of the independent review of the first two lines of defence, including other internal functions, units and business lines. The internal audit function performs its tasks fully independently of the other lines of defence.

38. To ensure their proper functioning, all internal control functions need to be independent of the business they control, have the appropriate financial and human resources to perform their tasks, have direct access and report directly to the management body in its supervisory function to raise concerns to and warn the supervisory function where appropriate. Within all three lines of defence, appropriate internal control procedures, mechanisms and processes should be designed, developed, maintained and evaluated under the ultimate responsibility of the management body.

39. All elements within the guidelines are subject to the principle of proportionality, meaning that they are to be applied in a manner that is appropriate, taking into account in particular the institution's size, internal organisation and nature, and the complexity of its activities.The principle of proportionality applies also to third-country branches. In this regard, the minimum requirements applicable to third-country branches should be relative to the risks that they pose to financial stability and market integrity in the EU and the Member States and should therefore depend on the classifcation of third-country branches as class 1 or class 2.

40. The guidelines specify further the requirements under Directive 2013/36/EU that need to be considered when setting up new structures, e.g. in third countries, including also offshore financial centres, and which aim to increase the transparency of and reduce the risks connected with such activities. Guidelines are also provided regarding the reporting of institutions on governance arrangements, including in relation to such structures.

41. The guidelines aim to establish a sound risk culture in institutions. Risks should be taken within a well-defined framework in line with the institution's risk strategy and risk appetite. This includes the establishment of and ensuring compliance with a system of limits and controls.

Risks within new products and business areas, but also risks that may result from changes to institutions' products, processes and systems, are to be duly identified, assessed, appropriately managed and monitored. The risk management function and compliance function should be involved in the establishment of the framework and the approval of such changes to ensure that all material risks are taken into account and that the institution complies with all internal and external requirements.

42. To ensure objective decision-making, oversight and compliance with external and internal requirements, including institutions' strategies and risk limits, institutions should implement a conflict-of-interest policy and internal whistleblowing procedures.

43. In order to prevent conflicts of interest, the management body should ensure that a framework for the identification and, where necessary, mitigation of conflicts of interests exist. The institution, its organisational substructures, staff and shareholders hold different interests that should be considered in such a framework in order to ensure that decisions are taken objectively. Examples of typical sources of conflicts of interests are diverging economic interests of different parties involved or close links between decision-makers and contractual parties.

44. The management body has the highest decision-making powers, consequently the identification and management of conflicts of interest of members of the management body and parties closely related to the members of the management body is a cornerstone of sound internal governance practices. Therefore, the guidelines specify measures that should be implemented by institutions to prudently manage conflicts of interests that may arise from granting loans to and entering into other transactions with members of the management body and their related parties.

EBA/CP/2025/XX

6 August 2025

Draft revised Guidelines on internal governance

Revisions made to EBA Guidelines on internal governance under CRD EBA/GL/2021/05 are shown in track changes

1. Compliance and reporting obligations

Status of these guidelines

1. These guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010[12]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions, including institutions, must make every effort to comply with the guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authority as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authority must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authority will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2021/05'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authority. Any change in the status of compliance must also be reported to EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3) of Regulation (EU) No 1093/2010.

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

2. Subject matter, scope and definitions

Subject matter

5. These guidelines specify further the internal governance arrangements, processes and mechanisms that institutions and third country branches, that are subject to Directive 2013/36/EU [13] and investment firms that are subject to Title VII of Directive 2013/36/EU in application of Article 1(2) and (5) of Regulation 2019/2033/EU, should implement in accordance with Article 74(1) and Article 48(g) of Directive 2013/36/EU to ensure their effective and prudent management.

Addressees

5a. These guidelines are addressed to competent authorities as defined in point (i) of Article 4 (2) of Regulation (EU) 1093/2010, and to financial institutions as defined in Article 4(1) of Regulation (EU) 1093/2010 that are either institutions for the purposes of the application of Directive 2013/36/EU as defined in point 3 of Article 3(1) of Directive 2013/36/EU ~~also having regard to Article 3 (3) of that Directive~~ or investment firms subject to Title VII of Directive 2013/36/EU in application of Article 1(2) and (5) of Regulation 2019/2033/EU ~~('institutions').~~('institutions'). These Guidelines are also addressed to third-country branches as defined in point 1 of Article 47(3) of Directive 2013/36/EU, and to financial holding companies and mixed financial holding companies that have been granted approval in accordance with Article 21a(1) of Directive 2013/36/EU also having regard to Article 3(3) of that Directive.

Scope of application

6. These guidelines apply in relation to institutions' governance arrangements, including their organisational structure and the corresponding lines of responsibility, processes to identify, manage, monitor and report all risks[14] they are or might be exposed to, ~~and~~the network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554 and the internal control framework.

7. The guidelines intend to embrace all existing board structures and do not advocate any particular structure. The guidelines do not interfere with the general allocation of competences in accordance with national company law. Accordingly, they should be applied irrespective of the board structure used (unitary and/or a dual board structure and/or

[13] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[14] Any reference to risks in these guidelines should include also money laundering and terrorist financing risks as well as environmental, social and governance risks, ~~including risks to climate change and biodiversity.~~ and risks in the context of artificial intelligence services.

another structure) across Member States. The management body, as defined in point~~s~~ (7~~) and (8)~~), of Article 3(1) of Directive 2013/36/EU~~,~~ should be understood as having management (executive) and supervisory (non-executive) functions as defined in points (8a) and (8) of that article[15].

8. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law. ~~When implementing these guidelines, competent authorities should take into account their national company law and specify, where necessary, to which body or members of the management body those functions should apply.~~

9. In Member States where the management body ~~delegates, partially or fully,~~appoints persons that effectively direct the ~~executive functions to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee),~~ business of the ~~persons who perform~~institutions, those ~~executive functions on the basis of that delegation should be understood as constituting~~persons belong in accordance with Article 3(1)(8a) of Directive 2013/36/EU to the management function of the management body~~. For the purposes of these guidelines, any reference~~ and are therefore to ~~the management body in its management function should be understood as including also the members of the executive body or the CEO, as defined~~be assessed for their suitability in ~~these guidelines, even if they have not been proposed or appointed as formal members of the institution's governing body or bodies under national law~~line with Article 91 of this Directive.

10. In Member States where some responsibilities are directly exercised by shareholders, members or owners of the institution instead of the management body, institutions should ensure that such responsibilities and related decisions are in line, as far as possible, with the guidelines applicable to the management body.

11. *deleted*

~~The definitions of CEO, chief financial officer (CFO) and key function holder used in these guidelines are purely functional and are not intended to impose the appointment of those officers or the creation of such positions unless prescribed by relevant EU or national law.~~

12. Institutions should comply and competent authorities should ensure that institutions comply with these guidelines on an individual, sub-consolidated and consolidated basis, in accordance with the level of application set out in Article 109 of Directive 2013/36/EU.

[15] See also recital 56 of Directive 2013/36/EU.

Definitions

13. Unless otherwise specified, terms used and defined in Directive 2013/36/EU and Regulation (EU) No 575/2013 have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

Risk appetite	means the aggregate level and types of risk an institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.
Risk capacity	means the maximum level of risk an institution is able to assume given its capital base, its risk management and control capabilities, and its regulatory constraints.
Risk culture	means an institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume.
Staff	means all employees of an institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to Directive 2013/36/EU, and all members of the management body in its management function and in its supervisory function.
Chief executive officer (CEO)	means the person who is responsible for managing and steering the overall business activities of an institution~~.~~ and is part of the management body in its management function.
~~**Chief financial officer (CFO)**~~	~~means the person who is overall responsible for managing all of the following activities: financial resources management, financial planning and financial reporting.~~
~~**Heads of internal control functions**~~	~~means the persons at the highest hierarchical level in charge of effectively managing the day-to-day operation of the independent risk management, compliance and internal audit functions.~~
~~**Key function holders**~~	~~means persons who have significant influence over the directionof the institution but who are neither members of themanagement body, nor the CEO. They include the heads ofinternal control functions and the CFO, where they are notmembers of the management body, and, where identified on a risk-based approach by institutions, other key function holders.~~ ~~Other key function holders might include heads of significantbusiness lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions.~~

Prudential consolidation	means the application of the prudential rules set out in Directive 2013/36/EU and Regulation (EU) No 575/2013 on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013.[16]
Gender pay gap	means the difference between the average gross hourly earnings of men and women expressed as a percentage of the average gross hourly earnings of men.
Consolidating institution	means an institution that is required to abide by the prudential requirements on the basis of the consolidated situation in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013.
Significant institutions	means institutions referred to in Article 131 of Directive 2013/36/EU (global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs)), and, as appropriate, other institutions determined by the competent authority or national law, based on an assessment of the institutions' size and internal organisation, and the nature, scope and complexity of their activities.
Listed institution	means institutions whose financial instruments are admitted to trading on a regulated market or on a multilateral trading facility as defined under Article 4(21) and Article 4(22) of Directive 2014/65/EU, in one or more Member States[17].
Shareholder	means a person who owns shares in an institution or, depending on the legal form of an institution, other owners or members of the institution.
Directorship	means a position as a member of the management body of an institution or another legal entity.
Operational resilience	means the ability of a financial entity to deliver critical or important functions through disruption. This ability enables a financial entity either directly or indirectly, through the use of functions provided by third-party service providers, to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical or important function through disruption .

[16] See also RTS on prudential consolidation under: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

[17] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

3. Implementation

Date of application

14. These guidelines apply from XX/XX/XXXX.

Amendment

15. The EBA Guidelines on internal governance (EBA/GL/2021/05) of 31 December 2021 are amended with effect from xx/xx/xxxx.

4. Guidelines

Title I – Proportionality

16. The proportionality principle encoded in Article 74(2) of Directive 2013/36/EU aims to ensure that internal governance arrangements are consistent with the individual risk profile and business model of the institution, so that the objectives of the regulatory requirements and provisions are effectively achieved.

17. Institutions should take into account their size and internal organisation, and the nature, scale and complexity of their activities, when developing and implementing internal governance arrangements. Significant institutions should have more sophisticated governance arrangements, while small and less complex institutions may implement simpler governance arrangements. Institutions should however note that the size or systemic importance of an institution may not, by itself, be indicative of the extent to which an institution is exposed to risks.

18. For the purpose of the application of the principle of proportionality and in order to ensure an appropriate implementation of the regulatory requirements and these guidelines, all the following aspects should be taken into account by institutions and competent authorities:

    a. the size in terms of the balance-sheet total of the institution and its subsidiaries within the scope of prudential consolidation;

    b. the geographical presence of the institution and the size of its operations in each jurisdiction;

    c. the legal form of the institution, including whether the institution is part of a group and, if so, the proportionality assessment for the group;

    d. whether it is a listed institution;

    e. whether the institution is authorised to use internal models for the measurement of capital requirements (e.g. the internal ratings-based approach);

    f. the type of authorised activities and services performed by the institution (e.g. see also Annex 1 to Directive 2013/36/EU and Annex 1 to Directive 2014/65/EU);

    g. the underlying business model and strategy; the nature and complexity of the business activities, and the institution's organisational structure;

h. the risk strategy, risk appetite and actual risk profile of the institution, taking into account also the result of the SREP capital and SREP liquidity assessments;

i. the ownership and funding structure of the institution;

j. the type of clients (e.g. retail, corporate, institutional, small businesses, public entities) and the complexity of the products or contracts;

k. the ~~outsourced~~use of third-party services providers (including the outsourcing of functions) and distribution channels;

l. the existing information and communication technology (ICT) systems, including continuity systems and ~~outsourcing functions~~the use of third party services providers in this area ; and

m. whether the institution falls under the definition in Points 145 and 146 of Article 4(1) of Regulation (EU) No 575/2013 of a small and non-complex institution or a large institution.

n. with respect to third country branches, whether they are qualifying third-country branches as defined under Article 48b of Directive 2013/36/EU or class 1 or class 2 in accordance with Article 48a of Directive 2013/36/ EU.

Title II – Role and composition of the management body and committees

1 Role and responsibilities of the management body

19. In accordance with Article 88(1) of Directive 2013/36/EU, the management body must have ultimate and overall responsibility for the institution and defines, oversees and is accountable for the implementation of the governance arrangements within the institution that ensure effective and prudent management of the institution.

20. The duties of the management body should be clearly defined, distinguishing between the duties of the management (executive) function and the supervisory (non-executive) function. The responsibilities and duties of the management body should be described in a written document and duly approved by the management body. All members of the management body should be fully aware of the structure and responsibilities of the management body, and of the division of tasks between different functions of the management body and its committees. Institutions should also draw up, maintain and update individual statements setting out the roles and duties of the members of the management body in its management function and a mapping of duties as specified under paragraphs 68a and 68b.

21. The management body in its supervisory function and in its management function should interact effectively. Both functions should provide each other with sufficient information to allow them to perform their respective roles. In order to have appropriate checks and balances in place, the decision-making within the management body should not be dominated by a single member or a small subset of its members.

22. The management body's responsibilities should include setting, approving and overseeing the implementation of:

    a. the overall business strategy and the key policies of the institution within the applicable legal and regulatory framework, taking into account the institution's long-term financial interests and solvency;

    b. the overall risk strategy, the institution's risk appetite and its risk management framework and measures to ensure that the management body devotes sufficient time to risk and risk management issues;

    c. an adequate and effective internal governance and internal control framework, as defined in Title V, that:

        i. includes a clear organisational structure and well-functioning ~~independent~~ internal risk management, compliance and audit functions that have sufficient authority, stature and resources to perform their functions;

        i. (a) includes effective processes to identify, manage, monitor and report the risks they are or might be exposed to, including ESG risks in the short, medium and long term, as well as concentration risk arising from exposures towards central counterparties;

        i. (b) network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554;

        ii. ensures compliance with applicable regulatory requirements in the context of the prevention of money laundering and terrorism financing;

    d. the amounts, types and distribution of both internal capital and regulatory capital to adequately cover the risks of the institution;

    e. targets for the liquidity management of the institution;

    f. a gender-neutral remuneration policy that, is in line with the remuneration principles set out in Articles 92 to 95 of Directive 2013/36/EU and the EBA guidelines on sound remuneration policies under ~~Articles 74(3) and 75(2) of~~ Directive 2013/36/EU[18] ~~and~~

[18] ~~EBA guidelines on sound remuneration policies~~

~~that takes~~, and promotes sound risk management taking into account the institution's risk appetite regarding ESG risks;

g. arrangements aimed at ensuring that the individual and collective suitability assessments of the management body are carried out effectively, that the composition and succession planning of the management body are appropriate, and that the management body performs its functions effectively[19];

h. a selection and suitability assessment process for key function holders[20];

i. arrangements aimed at ensuring the internal functioning of each committee of the management body, when established, detailing the:

    i. role, composition and tasks of each of them;

    ii. appropriate information flow, including the documentation of recommendations and conclusions, and reporting lines between each committee and the management body, competent authorities and other parties;

j. a risk culture in line with Section 9 of these guidelines, which addresses the institution's risk awareness and risk-taking behaviour;

k. a corporate culture and values in line with Section 10, which foster responsible and ethical behaviour, diversity and inclusion, including a code of conduct or similar instrument;

l. a conflict-of-interest policy at institutional level in line with Section 11 and for staff in line with Section 12; ~~and~~

m. arrangements aimed at ensuring the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards~~.~~; and

n. plans to monitor and address ESG risks in accordance with Article 76(2) of Directive 2013/36/EU as further specified by Section 6 of the EBA Guidelines on the management of ESG risks.

[19] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders.

[20] See also joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders.

o. specific plans and quantifiable targets in accordance with 76(2) of Directive 2013/36/EU to monitor and address the concentration risk arising from exposures towards systemic central counterparties.

23. When setting, approving and overseeing the implementation of the aspects listed in Paragraph 22 the management body should aim at ensuring a business model, governance arrangements, including a risk management framework that take into account all risks. When taking into account all risks institutions are exposed to, institutions should take into account all relevant risk factors, including ~~environmental, social~~the impact of ESG risks on traditional categories of financial and ~~governance risk factors.~~ non-financial risks in the short, medium and long ~~term Institutions should consider that their ESG risks may drive their prudential risks, including credit risks, e.g. via risk factors related to~~ term. This includes the ~~transition to a sustainable economy or external physical climate-related events that may affect debtors, market, liquidity,~~potential materialisation of operational and legal risks ~~and also reputational risks, e.g. via social and governance risk factors, e.g.~~ in the context of third party arrangements[21] including outsourcing arrangements[22] ~~and arrangements with third-party providers and subcontractors. Such risks include, e.g. legal risks in the~~ e.g. due to shortcomings in the area of contractual or labour law, ~~risks related to~~ potential human or fundamental rights violations or other ESG ~~risk~~ factors that may affect the country where a service provider is located and its ability to provide the agreed service levels.

24. The management body must oversee the process of disclosure and communications with external stakeholders and competent authorities.

25. All members of the management body should be informed about the overall activity, financial and risk situation of the institution, taking into account the economic environment, and about decisions taken that have a major impact on the institution's business.

26. *deleted*

~~A member of the management body may be responsible for an internal control function as referred to in Title V, Section 19.1, provided that the member does not have other mandates that would compromise the member's internal control activities and the independence of the internal control function.~~

27. The management body should monitor, periodically review and address any weaknesses identified regarding the implementation of processes, strategies and policies related to the responsibilities listed in Paragraphs 22 and 23. The internal governance framework and its implementation should be reviewed and updated on a periodic basis taking into account the

[21] Third party arrangements include subcontracting

[22] ~~See EBA report on ESG risk management and supervision published under the CRD Art. 98(8) for a description of EBA's understanding of ESG risks, transmission channels, and recommendations for arrangements, processes, mechanisms and strategies to be implemented by institutions to identify, assess and manage ESG risks.~~

proportionality principle, as further explained in Title I. A deeper review should be carried out where material changes affect the institution.

2 Management function of the management body

28. The management body in its management function should engage actively in the business of an institution and should take decisions on a sound and well-informed basis.

29. The management body in its management function should be responsible for the implementation of the strategies set by the management body and discuss regularly the implementation and appropriateness of those strategies with the management body in its supervisory function. The operational implementation may be performed by the institution's management.

29a. A member of the management body in its management function may be responsible for an internal control function as referred to in Title V, Sections 19.1 and 19.3, provided that the member does not have other mandates that would compromise the member's internal control activities and the independence of the internal control functions.

30. The management body in its management function should constructively challenge and critically review propositions, explanations and information received when exercising its judgement and taking decisions. The management body in its management function should comprehensively report, and inform regularly and where necessary without undue delay the management body in its supervisory function of the relevant elements for the assessment of a situation, the risks and developments affecting or that may affect the institution, e.g. material decisions on business activities and risks taken, the evaluation of the institution's economic and business environment, liquidity and sound capital base, and assessment of its material risk exposures.

31. Without prejudice to the national transposition of Directive 2015/849/EU, the management body should identify one of its members in line with the requirements under Article 46(4) of Directive 2015/849/EU Anti-Money Laundering Directive (AMLD) who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this directive, including the corresponding AML/CFT policies and procedures in the institution and at the level of the management body[23].

3 Supervisory function of the management body

32. The role of the members of the management body in its supervisory function should include monitoring and constructively challenging the strategy of the institution.

33. Without prejudice to national law the management body in its supervisory function should include independent members as provided for in Section 9.3 of the joint ESMA and EBA

[23] The management body as a collegial body remains responsible as a whole.

guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

34. Without prejudice to the responsibilities assigned under the applicable national company law, the management body in its supervisory function should:

    a. oversee and monitor management decision-making and actions and provide effective oversight of the management body in its management function, including monitoring and scrutinising its individual and collective performance and the implementation of the institution's strategy and objectives;

    b. constructively challenge and critically review proposals and information provided by members of the management body in its management function, as well as its decisions;

    c. taking into account the proportionality principle as set out in Title I, appropriately fulfil the duties and role of the risk committee, the remuneration committee and the nomination committee, where no such committees have been set up;

    d. ensure and periodically assess the effectiveness of the institution's internal governance framework and take appropriate steps to address any identified deficiencies;

    e. oversee and monitor that the institution's strategic objectives, organisational structure and risk strategy, its risk appetite and risk management framework, as well as other policies (e.g. remuneration policy) and the disclosure framework are implemented consistently;

    f. monitor that the risk culture of the institution is implemented consistently;

    g. oversee the implementation and maintenance of a code of conduct or similar code and effective policies to identify, manage and mitigate actual and potential conflicts of interest;

    h. oversee the integrity of financial information and reporting, and the internal control framework, including an effective and sound risk management framework;

    i. ensure that the heads of internal control functions are able to act independently and, regardless the responsibility to report to other internal bodies, business lines or units, can raise concerns and warn the management body in its supervisory function directly, where necessary, when adverse risk developments affect or may affect the institution; and

    j. monitor the implementation of the internal audit plan, after the prior involvement of the risk and audit committees, where such committees are established.

4 Role of the chair of the management body

35. The chair of the management body should lead the management body, contribute to an efficient flow of information within the management body and between the management body and the committees thereof, where established, and should be responsible for its effective overall functioning.

36. The chair should encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.

37. As a general principle, the chair of the management body should be a non-executive member. ~~Where the chair is permitted to assume executive duties, the institution should have measures in place to mitigate any adverse impact on the institution's checks and balances (e.g. by designating a lead board member or a senior independent board member, or by having a larger number of non-executive members within the management body in its supervisory function). In particular,~~ In accordance with Article 88(1)(e) of Directive 2013/36/EU, the chair of the management body in its supervisory function of an institution must not exercise simultaneously the functions of a CEO within the same institution.

38. The chair should set meeting agendas and ensure that strategic issues are discussed with priority. They should ensure that decisions of the management body are taken on a sound and well-informed basis and that documents and information are received in enough time before the meeting.

39. The chair of the management body should contribute to a clear allocation of duties between members of the management body and the existence of an efficient flow of information between them, in order to allow the members of the management body in its supervisory function to constructively contribute to discussions and to cast their votes on a sound and well-informed basis.

5 Committees of the management body in its supervisory function

5.1 Setting up committees

40. In accordance with Article 109(1) of Directive 2013/36/EU in conjunction with Articles 76(3), 88(2), and 95(1) of Directive 2013/36/EU, all institutions that are themselves significant, considering the individual, sub-consolidated and consolidated levels, must establish risk, nomination [24] and remuneration [25] committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this body. Non-significant institutions, including when they are within the scope of prudential consolidation of an

[24] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

[25] With regard to the remuneration committee, please refer to the EBA guidelines on sound remuneration practices.

institution that is significant in a sub-consolidated or consolidated situation, are not obliged to establish those committees.

41. Where no risk or nomination committee is established, the references in these guidelines to those committees should be construed as applying to the management body in its supervisory function, taking into account the principle of proportionality as set out in Title I.

42. Institutions may, taking into account the criteria set out in Title I of these guidelines, establish other committees (e.g. anti-money laundering/counter terrorist financing (AML/CTF), ethics, conduct and compliance committees).

43. Institutions should ensure a clear allocation and distribution of duties and tasks between specialised committees of the management body.

44. Each committee should have a documented mandate, including the scope of its responsibilities, from the management body in its supervisory function and establish appropriate working procedures.

45. Committees should support the supervisory function in specific areas and facilitate the development and implementation of a sound internal governance framework. Delegating to committees does not in any way release the management body in its supervisory function from collectively fulfilling its duties and responsibilities.

5.2 Composition of committees[26]

46. All committees should be chaired by a non-executive member of the management body who is able to exercise objective judgement.

47. Independent members[27] of the management body in its supervisory function should be actively involved in committees.

48. Where committees have to be set up in accordance with Directive 2013/36/EU or national law, they should be composed of at least three members.

49. Institutions should ensure, taking into account the size of the management body and the number of independent members of the management body in its supervisory function, that committees are not composed of the same group of members that forms another committee.

50. Institutions should consider the occasional rotation of chairs and members of committees, taking into account the specific experience, knowledge and skills that are individually or collectively required for those committees.

[26] This section should be read in conjunction with the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

[27] As defined in Section 9.3 of the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

51. The risk and nomination committees should be composed of non-executive members of the management body in its supervisory function of the institution concerned. The audit committee should be composed in accordance with Article 41 of Directive 2006/43/EC[28]. The remuneration committee should be composed in accordance with Section 2.4.1 of the EBA guidelines on sound remuneration policies[29]. Members of the remuneration ~~committee's composition~~ committee should ~~allow it~~have, individually and collectively, appropriate knowledge, skills and experience to ~~examine~~asses the ~~input~~impact of ESG factors on, and the consistency of the institution's risk appetite regarding ESG risks with, remuneration incentives ~~in relation to ESG factors~~ taking into account the assessment of the risk committee as ~~provided by the risk committee~~ specified under paragraph ~~65~~62.

52. In G-SIIs and O-SIIs, the nomination committee should include a majority of members who are independent and be chaired by an independent member. In other significant institutions, determined by competent authorities or national law, the nomination committee should include a sufficient number of members who are independent; such institutions may also consider as a good practice having a chair of the nomination committee who is independent.

53. Members of the nomination committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning the selection process and suitability requirements as set out under Directive 2013/36/EU.

54. In G-SIIs and O-SIIs, the risk committee should include a majority of members who are independent. In G-SIIs and O-SIIs the chair of the risk committee should be an independent member. In other significant institutions, determined by competent authorities or national law, the risk committee should include a sufficient number of members who are independent and the risk committee should be chaired, where possible, by an independent member. In all institutions, the chair of the risk committee should be neither the chair of the management body nor the chair of any other committee.

55. Members of the risk committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning risk management and control practices.

5.3 Committees' processes

56. Committees should regularly report to the management body in its supervisory function.

57. Committees should interact with each other as appropriate. Without prejudice to Paragraph 49, such interaction could take the form of cross-participation so that the chair or a member of a committee may also be a member of another committee.

[28] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87) as last amended by Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014.

[29] EBA guidelines on sound remuneration policies under ~~Articles 74(3) and 75(2) of~~ Directive 2013/36/EU ~~and disclosures under Article 450 of Regulation (EU) No 575/2013 (EBA/GL/2015/22).~~

58. Members of committees should engage in open and critical discussions, during which dissenting views are discussed in a constructive manner.

59. Committees should document the agendas of committee meetings and their main results and conclusions.

60. The risk and nomination committees should at least:

    a. have access to all relevant information and data necessary to perform their role, including information and data from relevant corporate and control functions (e.g. legal, finance, human resources, IT, internal audit, risk, compliance, including information on AML/CTF compliance and aggregated information on suspicious transaction reports, and ML/TF risk factors);

    b. receive regular reports, ad hoc information, communications and opinions from heads of internal control functions concerning the current risk profile of the institution, its risk culture and its risk limits, as well as on any material breaches[30], that may have occurred, with detailed information on and recommendations for corrective measures taken, to be taken or suggested to address them; periodically review and decide on the content, format and frequency of the information on risk to be reported to them; and

    c. where necessary, ensure the proper involvement of the internal control functions and other relevant functions (human resources, legal, finance) within their respective areas of expertise and/or seek external expert advice.

5.4 Role of the risk committee

61. Where established, the risk committee should at least:

    a. advise and support the management body in its supervisory function regarding the monitoring of the institution's overall actual and future risk strategy and risk appetite, taking into account all types of risks, to ensure that they are in line with the business strategy, objectives, corporate culture and values of the institution;

    b. assist the management body in its supervisory function in overseeing the implementation of the institution's risk strategy and the corresponding limits set;

    c. oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of an institution, such as market, credit, operational (including legal ~~and IT~~, fundamental rights, discrimination and ICT risks), and

[30] With regard to serious breaches in the area of AML/TF. Please refer also to the Guidelines EBA Guidelines on cooperation and information exchange between prudential supervisors , AML/CTF supervisors and financial intelligence units under Directive 2013/36/EU (EBA/GL/2021/15)~~to be issued under Article 117(6) of Directive 2013/36/EU, specifying the manner of cooperation and information exchange between the authorities referred to in Paragraph 5 of this article,~~ ,particularly in relation to cross-border groups and in the context of identifying serious breaches of anti-money laundering rules.

reputational risks, in order to assess their adequacy against the approved risk strategy and risk appetite;

d. provide the management body in its supervisory function with recommendations on necessary adjustments to the risk strategy resulting from, inter alia, changes in the business model of the institution, market developments or recommendations made by the risk management function;

e. provide advice on the appointment of external consultants that the supervisory function may decide to engage for advice or support;

f. review a number of possible scenarios, including stressed scenarios, to assess how the institution's risk profile would react to external and internal events;

g. oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the institution[31]. The risk committee should assess the risks associated with the offered financial products and services and take into account the alignment between the prices assigned to and the profits gained from those products and services; and

h. assess the recommendations of internal or external auditors and follow up on the appropriate implementation of measures taken.

62. The risk committee should collaborate with other committees whose activities may have an impact on the risk strategy (e.g. audit and remuneration committees) and regularly communicate with the institution's internal control functions, in particular the risk management function. The risk committee should provide input to the remuneration committee regarding ESG ~~risk factors~~risks and related targets or key performance indicators that should be taken into account in the remuneration policy and for performance measurement.

63. When established, the risk committee must, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration policies and practices take into consideration the institution's risk, capital and liquidity and the likelihood and timing of earnings.

[31] See also the EBA guidelines on product oversight and governance arrangements for retail banking products, available at http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

5.5 Role of the audit committee

64. In accordance with Directive 2006/43/EC[32], where established, the audit committee should, inter alia:

a. monitor the effectiveness of the institution's internal quality control and risk management systems and, where applicable, its internal audit function, with regard to the financial reporting of the audited institution, without breaching its independence;

b. oversee the establishment of accounting policies by the institution;

c. monitor the financial reporting process and submit recommendations aimed at ensuring its integrity;

d. review and monitor the independence of the statutory auditors or the audit firms in accordance with Articles 22, 22a, 22b, 24a and 24b of Directive 2006/43/EU and Article 6 of Regulation (EU) No 537/2014[33], and in particular the appropriateness of the provision of non-audit services to the audited institution in accordance with Article 5 of that regulation;

e. monitor the statutory audit of the annual and consolidated financial statements, in particular its performance, taking into account any findings and conclusions by the competent authority pursuant to Article 26(6) of Regulation (EU) No 537/2014;

f. be responsible for the procedure for the selection of external statutory auditor(s) or audit firm(s) and recommend for approval by the institution's competent body their appointment (in accordance with Article 16 of Regulation (EU) No 537/2014 except when Article 16(8) of Regulation (EU) No 537/2014 is applied), compensation and dismissal;

g. review the audit scope and frequency of the statutory audit of annual or consolidated accounts;

h. in accordance with Article 39(6)(a) of Directive 2006/43/EU, inform the administrative or supervisory body of the audited entity of the outcome of the statutory audit and explain how the statutory audit contributed to the integrity of financial reporting and what the role of the audit committee was in that process; and

[32] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87), as last amended by Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014.

[33] Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC (OJ L 158, 27.5.2014, p. 77).

i. receive and take into account audit reports.

5.6 Combined committees

65. In accordance with Article 76(3) of Directive 2013/36/EU, competent authorities may allow institutions that are not considered significant to combine the risk committee with, where established, the audit committee as referred to in Article 39 of Directive 2006/43/EC.

66. Where risk and nomination committees are established in non-significant institutions, they may combine the committees. If they do so, those institutions should document the reasons why they have chosen to combine the committees and how the approach achieves the objectives of the committees.

67. Institutions should at all times ensure that the members of a combined committee possess, individually and collectively, the necessary knowledge, skills and expertise to fully understand the duties to be performed by the combined committee[34].

Title III – Governance framework

6 Organisational framework and structure

6.1 Organisational framework

68. The management body of an institution should ensure a suitable and transparent organisational and operational structure for that institution and should have a written description of it. The structure should promote and demonstrate the effective and prudent management of an institution at individual, sub-consolidated and consolidated levels. The management body should ensure that the internal control functions are independent of the business lines they control, including that there is an adequate segregation of duties, and that they have the appropriate financial and human resources as well as powers to effectively perform their role. ~~The reporting lines and the allocation of responsibilities, in particular amongkey function holders, within an institution should be clear, well-defined, coherent, enforceable and duly documented. The documentation should be updated as appropriate.~~ It should ensure that institutions maintain at all times sufficient substance to satisfy the conditions of their authorisation as defined by Commission Delegated Regulation (EU) 2022/2580 and Commission Implementing Regulation (EU) 2022/2581, and do not become 'empty shells' or 'letter-box entities', including when using third-party arrangements, or executing back-to-back transactions or any other service agreement with their head undertaking if applicable.

68a. Mapping of duties:

[34] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

a. Institutions should draw up and maintain, in accordance with Article 88(3) of Directive 2013/36/EU, in a single set of documents or a repository, an accurate and comprehensive mapping of duties including details of the reporting lines, of the lines of responsibility, and of the persons who are part of the governance arrangements as referred to in Article 74(1) of Directive 2013/36/EU and of their duties.

b. In accordance with Article 109 of Directive 2013/36/EU, these guidelines should also apply on an individual, sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation. The mapping of duties should be drawn at entity level, therefore each institution within a group should draw up a mapping. The consolidating institution should additionally draw up a mapping of duties at consolidated level and should ensure that the consolidated-level mapping is accurate and updated, including by receiving upon request the necessary information from the institutions and investment firms within the group. In addition, institutions which are part of a group should receive from the consolidating institution the necessary information relevant for the mapping of duties at the individual institution level.

c. The management body should agree and set out clearly where duties lie for the role of each individual member and what those duties entail. The duties should be outlined separately for both the management and the supervisory function of the management body. The management body should be responsible for the allocation of the duties and responsibilities assigned to senior management and key function holders even if those duties are drafted below management body level.

~~a.~~d. The mapping of duties should enable the institution to identify any gaps between the roles and the activities covered by the institution and ensure an effective internal governance framework. Institutions should be responsible for developing and maintaining a mapping of duties that is appropriate for, and accurately reflects the size and nature, organisational structure and complexity of the institution including, where applicable, of the group.

e. The mapping of duties should be coherent with the individual statements of role and duties as referred to in paragraph 68b. It should (i) provide a clear overview how roles and duties allocated in a particular statement fit into the overall management system and internal governance; and (ii) include sufficient information to enable a clear understanding of how the management and internal governance arrangements of the institution are structured and operate.

f. The mapping of duties should complement the institution's existing governance framework, which explains its governance arrangements, how its governing bodies are structured and interact, and its organisational chart, and in addition include at least the following:

    i. a description of key aspects of the institution's activities, business areas and management functions including internal control functions, how each aspect relates to the overall governance of the institution and details of the reporting lines and lines of duty;

ii. how the management body in its management function, the management body in its supervisory function and its sub-committees contribute to the decision making of the management body or bodies;

~~i.~~iii. the names of all members of the management body, senior management and KFH and a summary of their roles and duties consistent with the individual statements of duties;

iv. the details of the reporting lines of the members of the management body in its management function, senior management and key function holders, including their relationships with committees within the institution and, if applicable, other institutions of the group;

v. a rationale for any roles and duties that are shared;

vi. in case an institution uses third-party arrangements including outsourcing, details of who is responsible for the outsourced function or the function provided by the third-party service provider in accordance with paragraph 45c of the EBA guidelines on the sound management of third-party risk.

g. The management body should approve the mapping of duties and institutions should timely update it as appropriate, taking also into account the review of the individual statements. It should be made available at least to all members a of the management body and key function holders and submitted to the competent authorities in due time upon request. In two-tier-structures, the management body in its supervisory function should approve the mapping of duties.

68b. Individual statements of roles and duties

a. Institutions should ensure that each member of the management body in its management function, senior management and KFH has a documented statement of role and duties which clearly sets out their role. The statement shall therefore indicate the key duties which have been allocated to them and should be consistent with the mapping of duties. Institutions should ensure that the description provided is concise, logical, but sufficiently detailed to make it understandable. The description may include an indication of the time commitment expected to fulfil the duties. Institutions may use the template provided in Annex II.

b. The allocation in the individual statements of role(s) and duties to a member of the management body in its management function does not exempt the respective individuals from their roles and duties as members of the management body. All members of the management body in its management function are expected to have an appropriate understanding of, and contribute to, areas of the business, including for any other roles and duties not directly attributed to the respective member. Moreover, even when roles and duties are allocated to a specific individual, the other members of the management body should not be exempted from their collective duty regarding the institution.

c. If a member of the management body in its management function, a member of senior management or a key function holder holds more than one role within the institution

that is concerned by the statement, only one statement of roles and duties is required. In the case of an individual who holds roles in more than one institution, including within a group, an individual statement is required in respect to each institution.

d. The individual statement of roles and duties should be submitted to the competent authorities in accordance with the RTS to further specify the minimum content of the suitability questionnaire, curricula vitae and the internal suitability assessment to be submitted to the competent authorities for conducting the suitability assessment mandated under Article 91(10 of Directive 2013/36/EU or upon request, in due time. It should be kept up-to-date and be signed in physical or electronic form by the respective individual it applies to. Institutions should review it on a regular basis, taking into account the review of the mapping of duties.

68c. An individual is found to not be fulfilling their duties listed in their individual statement if an issue is detected in one of their duties or areas they are responsible for, and the individual is has not taken the actions that could reasonably be expected from them to prevent the issue from occurring or continuing to occur once brought to their attention. The institution should take appropriate measures to ensure that all individuals appropriately fulfil their duties, and the individuals should be able to demonstrate to the supervisor upon request that they have taken all actions in their position that could reasonably be expected from them.

69. The organisational structure of the institution should not impede the ability of the management body to oversee and manage effectively the risks the institution or the group faces or the ability of the competent authority to effectively supervise the institution.

70. The management body should assess whether and how material changes to the group's structure (e.g. setting up of new subsidiaries, mergers and acquisitions, selling or winding-up parts of the group, or external developments) impact the soundness of the institution's organisational framework. Where weaknesses are identified, the management body should make any necessary adjustments swiftly.

6.2 Know your structure

71. The management body should fully know and understand the legal, organisational and operational structure of the institution ('know your structure') and ensure that it is in line with its approved business and risk strategy and risk appetite and covered by its risk management framework.

72. The management body should be responsible for the approval of sound strategies and policies for the establishment of new structures. Where an institution creates many legal entities within its group, their number and, in particular, the interconnections and transactions between them should not pose challenges for the design of its internal governance, and for the effective management and oversight of the risks of the group as a whole. The management body should ensure that the structure of an institution and, where applicable, the structures within a group, taking into account the criteria specified in Section 7, are clear,

efficient and transparent to the institution's staff, shareholders and other stakeholders and to the competent authority.

73. The management body should guide the institution's structure, its evolution and its limitations and should ensure that the structure is justified and efficient and does not involve undue or inappropriate complexity.

74. The management body of a consolidating institution should understand not only the legal, organisational and operational structure of the group but also the purpose and activities of its different entities and the links and relationships among them. This includes understanding group-specific operational risks and intra-group exposures as well as how the group's funding, capital, liquidity and risk profiles could be affected under normal and adverse circumstances. The management body should ensure that the institution is able to produce information on the group in a timely manner, regarding the type, the characteristics, the organisational chart, the ownership structure and the businesses of each legal entity, and that the institutions within the group comply with all supervisory reporting requirements on an individual, sub-consolidated and consolidated basis.

75. The management body of a consolidating institution should ensure that the different group entities (including the consolidating institution itself) receive enough information to get a clear perception of the general objectives, strategies and risk profile of the group and how the group entity concerned is embedded in the group's structure and operational functioning. Such information and revisions thereof should be documented and made available to the relevant functions concerned, including the management body, business lines and internal control functions. The members of the management body of a consolidating institution should keep themselves informed about the risks the group's structure causes, taking into account the criteria specified in Section 7 of the guidelines. This includes receiving:

    a. information on major risk drivers;

    b. regular reports assessing the institution's overall structure and evaluating the compliance of individual entities' activities with the approved group-wide strategy; and

    c. regular reports on topics where the regulatory framework requires compliance at individual, sub-consolidated and consolidated levels.

6.3 Complex structures and non-standard or non-transparent activities

76. Institutions should avoid setting up complex and potentially non-transparent structures. Institutions should take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with

money laundering, terrorist financing or other financial crimes and the respective controls and legal framework in place[35]. To this end, institutions should take into account at least:

a. the extent to which the jurisdiction in which the structure will be set up complies effectively with EU and international standards on tax transparency, anti-money laundering and countering the financing of terrorism[36];

b. the extent to which the structure serves an obvious economic and lawful purpose;

c. the extent to which the structure could be used to hide the identity of the ultimate beneficial owner;

d. the extent to which the customer's request that leads to the possible setting up of a structure gives rise to concern;

e. whether the structure might impede appropriate oversight by the institution's management body or the institution's ability to manage the related risk; and

f. whether the structure poses obstacles to effective supervision by competent authorities.

77. In any case, institutions should not set up opaque or unnecessarily complex structures which have no clear economic rationale or legal purpose or structures that could raise concerns that these might be created for a purpose connected with financial crime.

78. When setting up such structures, the management body should understand them and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. Such structures should be approved and maintained only when their purpose has been clearly defined and understood, and when the management body is satisfied that all material risks, including reputational risks, have been identified, that all risks can be managed effectively and appropriately reported, and that effective oversight has been ensured. The more complex and opaque the organisational and operational structure, and the greater the risks, the more intensive the oversight of the structure should be.

79. Institutions should document their decisions and be able to justify their decisions to competent authorities.

80. The management body should ensure that appropriate actions are taken to avoid or mitigate the risks of activities within such structures. This includes ensuring that:

[35] For further details on the assessment of country risk and the risk associated with individual products and customers, institutions should refer also to the joint guidelines on ML/TF risk factors (EBA GL JC/2017/37) currently under review.

[36] See also: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

a. the institution has in place adequate policies and procedures and documented processes (e.g. applicable limits, information flows) for the consideration, compliance, approval and risk management of such activities, taking into account the consequences for the group's organisational and operational structure, its risk profile and its reputational risk;

b. information concerning these activities and the risks thereof is accessible to the consolidating institution and internal and external auditors and is reported to the management body in its supervisory function and to the competent authority that granted authorisation; and

c. the institution periodically assesses the continuing need to maintain such structures.

81. These structures and activities, including their compliance with legislation and professional standards, should be subject to regular review by the internal audit function following a risk-based approach.

82. Institutions should take the same risk management measures as for the institution's own business activities when they perform non-standard or non-transparent activities for clients (e.g. helping clients to set up vehicles in offshore jurisdictions, developing complex structures, financing transactions for them or providing trustee services) that pose similar internal governance challenges and create significant operational and reputational risks. In particular, institutions should analyse the reason why a client wants to set up a particular structure.

7 Organisational framework ~~in a group context~~

7.1 Application in a group context

83. In accordance with Article 109(2) of Directive 2013/36/EU, parent undertakings and subsidiaries subject to that directive should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated or sub-consolidated basis. To this end, parent undertakings and subsidiaries within the scope of prudential consolidation should implement such arrangements, processes and mechanisms in their subsidiaries not subject to Directive 2013/36/EU, including those established in third countries, including in offshore financial centres, to ensure robust governance arrangements on a consolidated and sub-consolidated basis. With regard to remuneration requirements some exceptions in line with Article 109 (4) and (5) apply[37]. Competent functions within the consolidating institution and its subsidiaries should interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms should ensure that the consolidating institution has sufficient data and information and is able to assess the group-wide risk profile, as detailed in Section 6.2.

[37] Please refer also to the EBA guidelines on sound remuneration policies

84. The management body of a subsidiary that is subject to Directive 2013/36/EU should adopt and implement on the individual level the group-wide governance policies established at the consolidated or sub-consolidated level, in a manner that complies with all specific requirements under EU and national law.

85. At the consolidated and sub-consolidated levels, the consolidating institution should ensure adherence to the group-wide governance policies and internal control framework as referred to in Title V by all institutions and other entities within the scope of prudential consolidation, including their subsidiaries not themselves subject to Directive 2013/36/EU. When implementing governance policies, the consolidating institution should ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

86. A consolidating institution should consider the interests of all its subsidiaries, and how strategies and policies contribute to the interest of each subsidiary and the interest of the group as a whole over the long term.

87. Parent undertakings and their subsidiaries should ensure that the institutions and entities within the group comply with all specific regulatory requirements in any relevant jurisdiction.

88. The consolidating institution should ensure that subsidiaries established in third countries, and which are included in the scope of prudential consolidation, have governance arrangements, processes and mechanisms in place that are consistent with group-wide governance policies and comply with the requirements of Articles 74 to 96 of Directive 2013/36/EU and these guidelines, as long as this is not unlawful under the laws of the third country.

89. The governance requirements of Directive 2013/36/EU and provisions in these guidelines apply to institutions independent of the fact that they may be subsidiaries of a parent undertaking in a third country. Where an EU subsidiary of a parent undertaking in a third country is a consolidating institution, the scope of prudential consolidation does not include the level of the parent undertaking located in a third country and other direct subsidiaries of that parent undertaking. The consolidating institution should ensure that the group-wide governance policy of the parent institution in a third country is taken into consideration within its own governance policy insofar as this is not contrary to the requirements set out under relevant EU law, including Directive 2013/36/EU and the further specifications in these guidelines.

89a. Subsidiaries of third-country undertakings should maintain at all times sufficient substance to satisfy the conditions of their authorisation as defined by Commission Delegated Regulation (EU) 2022/2580 and Commission Implementing Regulation (EU) 2022/2581), and not become ‘empty shells’ or ‘letter-box entities’, including when using third-party

arrangements, or executing back-to-back transactions or any other service agreement with their head undertaking.

90. When establishing policies and documenting governance arrangements, institutions should take into account the aspects listed in Annex I to the guidelines. While policies and documentation may be included in separate documents, institutions should consider combining them or referring to them in a single governance framework document.

7.2 Third-country branches' internal governance arrangements

90a. Third-country branches should implement a robust and sound governance framework in accordance with Articles 48g and 74 of Directive 2013/36/EU, as a general principle, in the same way as institutions, taking into account the criteria for the application of the proportionality set out in Title I. When applied to third-country branches, references to the management body in its supervisory function should be understood as the management body in its supervisory function of the head undertaking.

90b. The two persons or more located in the relevant Member State effectively directing the business of third-country branches required by Article 48g of Directive 2013/36/EU should have the same duties and responsibilities as the members of the management body in its management function referred to in paragraphs 28 to 31 where applicable. The reporting towards the management body in its supervisory function referred to in paragraph 30 should be carried out by the local management of the third-country branch towards the supervisory function of the head undertaking, either directly or through the management function of the head undertaking. Taking into account the criteria for the application of proportionality under Title I, Class 1 third-country branches may establish or be required by competent authorities to establish a local management committee to ensure an adequate governance. In this case, the local management committee should be composed of individuals having the same tasks and duties as the management body in its management function as referred to in paragraphs 28 to 31 where applicable, and it should comply with the open discussion and documentation requirements referred to in paragraphs 58 and 59.

90c. The persons effectively directing the business of third-country branches or the members of the local management committee should be able to commit sufficient time to fulfill their roles and functions at the branch level, regardless of whether these persons have to fulfill equivalent roles for the head office in the third country or another group entity or third-country branch. Where this is the case, it is essential that conflicts of interest arising from such equivalent roles are avoided or managed to ensure that their responsibilities at branch level are not compromised. They should be sufficiently present in the Member State and in the premises of the third-country branch to effectively fulfil their role and the working arrangements in third-country branches should not impede or render unverifiable the presence in the relevant Member State of the persons effectively directing the business of the branch. The position held in the third-country branch should be counted, where the conditions of Article 91 paragraphs (3) and (4) of Directive 2013/36/EU are met, as an

executive directorship. They should not hold positions as heads of internal control functions within the head undertaking.

90d. The persons effectively directing the business of the third-country branch, the members of the local management committee where applicable, and their key function holders, including the heads of the internal control functions, should possess good repute, sufficient knowledge, skills and experience to perform their duties as set out in the Joint EBA and ESMA Guidelines on the assessment of the suitability of members of the management body and key function holders.

90e. In line with Article 76(6) of Directive 2013/36/EU, the heads of the internal risk management, compliance and audit functions of class 1 third-country branches, and of class 2 third-country branches if required by the competent authority in accordance with Article 48g(3) of directive 2013/36 EU, should not be removed without prior approval of the management body in its supervisory function of the third-country head undertaking.

90f. Where third country-branches are required to apply the requirements of Article 76(6) third and fifth subparagraphs and combine the function of head of risk management or compliance with other functions under the responsibility of a senior person, they should be able to demonstrate that the nature, scale and complexity of the activities of the branch do not justify appointing a specific person for the risk management function or the compliance function and that the assessment of conflicts of interests required under Article 76(6) 3rd subparagraph has been performed. The decision should be documented.

90g. Third-country branches should maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities', including when using third-party arrangements, or executing back-to-back transactions or any other service agreement with their head undertaking. To this end, they should:

a. meet all the conditions of their authorisation under Article 48(c) of Directive 2013/36/EU at all times, including the at least two persons effectively directing the business or the members of the local management committee carrying out their duties and responsibilities as set out in paragraphs 28 to 31 of these guidelines;

b. retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements;

c. exercise appropriate oversight of operational tasks of internal control functions that are provided by a third party service provider, and be able to manage the risks that are generated by the use of third-party service providers performing or supporting critical or important functions; and

d. have sufficient resources and capacities to ensure compliance with points (a) to (c).

The use of third-party arrangements including intragroup arrangements and third-party service providers located in third countries , should be made in an orderly manner and to an extent that does not undermine third-country branches' capabilities to meet the conditions for authorisation.

90h. Third-country branches should manage their ICT risks in accordance with Article 48g (4) of Directive 2013/36/EU and Regulation (EU) 2022/2554 (DORA). ICT third-party arrangements should be duly documented and filed within a register in accordance with DORA and Commission Implementing Regulation (EU) 2024/2956[38].

90i. When relying on back-to-back booking arrangements, third country branches should ensure at a minimum, that transactions with an EU nexus are neither systematically nor substantially back-to-backed, and are risk-managed from the EU. Accordingly, the associated business is expected to be run in the Member State. Third-country branches should be able to actively manage the risks linked to back-to-back booking arrangements and remote booking arrangements, e.g. counterparty credit risk, CVA risk, settlement risk.

90j. Third-country branches should comply with the remuneration principles set out in Articles 92 to 95 of Directive 2013/36/EU[39] and the EBA guidelines on sound remuneration policies under Directive 2013/36/EU, taking into account the branche's risk appetite regarding ESG risks. Third country branches should be able to demonstrate whether committees as referred to in Title II or an equivalent mechanism have been established at group level, including the remuneration committee as referred to in the Guidelines on sound remuneration under Directive 2013/36/EU, and provide all the necessary information and documents where necessary to ensure that gender-neutral remuneration principles are being complied with.

8 ~~Outsourcing~~Third-party risk management policy [40]

91. The management body should approve and regularly review and update the ~~outsourcing~~ third-party risk management policy of an institution ~~in line with Article 28(12) of Regulation (EU) 2022/2554~~[41], ensuring that appropriate changes are implemented in a timely manner.

92. The ~~outsourcing~~ third-party risk management policy [42] should consider the impact of ~~subcontracting~~third-party arrangements including outsourcing arrangements on an institution's business and the risks it faces (such as operational risks, including legal and ICT risks; reputational risks; and concentration risks). The policy should include the reporting and monitoring arrangements to be implemented from inception to the end of ~~an outsourcing agreement~~a third-party arrangement (including drawing up the business case for ~~outsourcing,~~

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1733138247253&uri=CELEX%3A32024R2956

[39] TCB are also subject to the reporting requirements set out in GL on the data collection exercises regarding high earners under Directive 2013/36/EU and under Directive (EU) 2019/2034.

[40] See also: EBA Guidelines on ~~outsourcing arrangements~~the sound management of third party risk available at:

[41] For ICT, see Article 28(10) of Regulation(EU) 2022/2054

[42] Third-party risk includes the use of subcontractors by the direct third-party service providers.

~~entering into an outsourcing contract~~the third-party arrangement, the implementation of the contract to its expiry, ~~contingency~~business continuity plans and exit strategies). An institution remains fully responsible for all ~~outsourced~~ services and activities provided by third-party services providers and management decisions arising from them. Accordingly, the ~~outsourcing~~ third-party risk management policy should make it clear that ~~outsourcing does~~third-party arrangements do not relieve the institution of its legal and regulatory obligations and of its responsibilities to its customers and must be consistent with all other legislatives and regulatory requirements the institution is subject to.

93. The policy should state that ~~outsourcing~~ third-party arrangements should not hinder effective on-site or off-site supervision of the institution and should not contravene any supervisory restrictions on services and activities. The policy should also cover intragroup ~~outsourcing~~ third-party arrangements (i.e. services provided by a separate legal entity within an institution's group) and take into account any specific group circumstances.

Title IV – Risk culture and business conduct

9 Risk culture

94. A sound, diligent and consistent risk culture should be a key element of institutions' effective risk management and should enable institutions to make sound and informed decisions. Institutions should also aim, as part of the risk culture, at establishing a culture of equality, diversity and inclusion and prevent discrimination and harassment.

95. Institutions should develop an integrated and institution-wide risk culture, based on a full understanding and holistic view of the risks they face and how they are managed, taking into account the institution's risk appetite.

96. Institutions should develop a risk culture through policies, communication and staff training regarding the institutions' activities, strategy and risk profile, and should adapt communication and staff training to take into account staff's responsibilities regarding risk-taking and risk management.

97. Staff should be fully aware of their responsibilities relating to risk management. Risk management should not be confined to risk specialists or internal control functions. Business units, under the oversight of the management body, should be primarily responsible for managing risks on a day-to-day basis in line with the institution's policies, procedures and controls, taking into account the institution's risk appetite and risk capacity.

98. A strong risk culture should include but is not necessarily limited to:

    a. Tone from the top: the management body should be responsible for setting and communicating the institution's core values and expectations. The behaviour of its members should reflect the values. Institutions' management, including key function holders, should contribute to the internal communication of core values and

expectations to staff. Staff should act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance within or outside the institution (e.g. to the competent authority through a whistleblowing process). The management body should on an ongoing basis promote, monitor and assess the risk culture of the institution; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the institution; and make changes where necessary.

b. Accountability: relevant staff at all levels should know and understand the core values of the institution and, to the extent necessary for their role, its risk appetite and risk capacity. They should be capable of performing their roles and be aware that they will be held accountable for their actions in relation to the institution's risk-taking behaviour.

c. Effective communication and challenge: a sound risk culture should promote an environment of open communication and effective challenge in which decision-making processes encourage a broad range of views, allow for testing of current practices, stimulate a constructive critical attitude among staff, and promote an environment of open and constructive engagement throughout the entire organisation.

d. Incentives: appropriate incentives should play a key role in aligning risk-taking behaviour with the institution's risk profile and its long-term interest[43].

10 Corporate values and code of conduct

99. The management body should develop, adopt, adhere to and promote high ethical and professional standards, taking into account the specific needs and characteristics of the institution, and should ensure the implementation of such standards (through a code of conduct or similar instrument). It should also oversee adherence to these standards by staff. Where applicable, the management body may adopt and implement the institution's group-wide standards or common standards released by associations or other relevant organisations.

100. Institutions should ensure that there is no discrimination of staff based on gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

101. Institution's policies should be gender neutral. This includes, but is not limited to remuneration, recruitment policies, career development and succession plans, access to training and ability to apply for internal vacancies. Institutions should ensure equal

[43] Please refer also to the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU ~~and disclosures under Article 450 of Regulation (EU) No 575/2013 (EBA/GL/2015/22~~(EBA/GL/2021/04), available at https://www.eba.europa.eu/regulation-and-policy/remuneration.

opportunities[44] for all staff independent of their genders, including with regard to career perspectives and aim to improve the representation of the underrepresented gender in positions within the management body as well as in the group of staff that have managerial responsibilities as defined in the Commission's Delegated Regulation (regulatory technical standards (RTS) on identified staff).[45] Where the recruitment process includes selection committees, those should have as a general principle a gender -balanced compo~~i~~sition. Institutions should monitor the development of the gender pay-gap separately for identified staff (excluding members of the management body), members of the management body in its management function, members of the management body in the supervisory function and other staff. Institutions should have policies that foster gender neutrality in maternity and paternity leave access and duration, and that facilitate the reintegration of staff after maternity, paternity or parental leave.

101a. Institutions should use additional indicators to monitor the development of the representation and equal treatment of staff of different genders and take the results of their monitoring into account within their approach to manage staff. Such indicators might include:

a. representation of genders at different management levels, including management body and senior management;

b. representation of genders on committees;

c. representation of genders in identified staff and all staff;

d. representation of genders per business/support area;

e. age distribution by gender, in particular for managerial positions;

f. ratio of temporary and permanent contracts by gender;

g. ratio of full-time vs part-time positions per gender;

h. representation of genders in succession planning for managerial positions;

i. days of training by gender;

j. entries and exits / staff turnover by gender;

k. complaints of staff regarding discrimination, harassment or equal pay issues per gender.

102. The implemented standards should aim at enhancing the institution's robust governance arrangements and reducing the risks to which the institution is exposed, ~~in particular~~including

[44] See also Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation

[45] See also EBA Guidelines on gender neutral remuneration policies

ESG risks. The professional standards should also aim at reducing in particular operational and reputational risks, which can have a considerable adverse impact on an institution's profitability and sustainability through fines, litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties, and the loss of brand value and consumer confidence.

103. The management body should have clear and documented policies for how these standards should be met. These policies should:

a. remind staff that all the institution's activities should be conducted in compliance with the applicable law and with the institution's corporate values;

b. promote risk awareness through a strong risk culture in line with Section 9 of the guidelines, conveying the management body's expectation that activities will not go beyond the defined risk appetite and limits defined by the institution and the respective responsibilities of staff;

c. set out principles on and provide examples of acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, economic and financial crime including but not limited to fraud, money laundering and terrorist financing (ML/TF), anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws, tax offences, whether committed directly or indirectly, including through unlawful or banned dividend arbitrage schemes;

d. clarify that in addition to complying with legal and regulatory requirements and internal policies, staff are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; and

e. ensure that staff are aware of the potential internal and external disciplinary actions, legal actions and sanctions that may follow misconduct and unacceptable behaviours.

104. Institutions should monitor compliance with such standards and ensure staff awareness, e.g. by providing training. Institutions should define the function responsible for monitoring compliance with and evaluating breaches of the code of conduct or similar instrument and a process for dealing with issues of non-compliance. The results should periodically be reported to the management body.

11 Conflict of interest policy at institutional level

105. The management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at institutional level, e.g. as a result of the various activities and roles of the institution, of different institutions within the

scope of prudential consolidation or of different business lines or units within an institution, or with regard to external stakeholders.

106. Institutions should take, within their organisational and administrative arrangements, adequate measures to prevent conflicts of interest from adversely affecting the interests of its clients.

107. Institutions' measures to manage or, where appropriate, mitigate conflicts of interest should be documented and include, inter alia:

a. an appropriate segregation of duties, e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons;

b. establishing information barriers, e.g. through the physical separation of certain business lines or units.

107a. In accordance with article 88 paragraph 1 of Directive 2013/36/EU, the simultaneous exercise within the same institution of the functions of chair of the management body in its supervisory function and CEO is prohibited. Similarly, within a group, the role of Chair of the management body in its supervisory function of a parent entity should not be held by the CEO of a subsidiary. Besides, the simultaneous exercise of the role of member of the management body in its management function and of member of the management body in its supervisory function in different institutions that are part of the same group should be assessed regarding potential conflicts of interests stemming in particular from the individual's duty to oversee their own previous actions and if detected, they should be properly mitigated.

107b. Where it is decided that the CEO will, after their executive directorship ended, become a member of the management body in its supervisory function (including Chair), and the individual is not subject to a cooling-off period lasting 3 years or more, institutions should have measures in place to mitigate any potential conflict of interest, stemming in particular from the individual's duty to oversee, as non-executive member of the management body, their own previous actions as CEO, which may include, but are not limited to, the following illustrative actions, without prejudice to national law:

a. The chair who previously was a CEO will not chair the management body discussion when an item is being discussed which is identified as a significant professional conflict of interest.

b. If deemed necessary, the chair or non-executive member who previously held the CEO role may be requested by the other members of the management body in its supervisory function to abstain from voting for such items.

c. In cases when the discussion or decision refers to the evaluation of their former performance as CEO, or refers to remuneration resolutions for their previous function, the chair or non-executive member cannot participate in the discussion, nor take part in the vote.

Institutions should consider implementing similar appropriate measures in cases where a member of the management body in its management function other than the CEO is to become a member of the management body in its supervisory function and the individual is not subject to a cooling-off period lasting 3 years or more.

12 Conflict of interest policy for staff[46]

108. The management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts between the interests of the institution and the private interests of staff, including members of the management body, which could adversely influence the performance of their duties and responsibilities. A consolidating institution should consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.

109. The policy should aim at identifying conflicts of interest of staff, including the interests of their closest family members. Institutions should take into consideration that conflicts of interest may arise not only from present but also from past personal or professional relationships. Where conflicts of interest arise, institutions should assess their materiality and decide on and implement mitigating measures, as appropriate.

110. Regarding conflicts of interest that may result from past relationships, institutions should set an appropriate timeframe for which they want staff to report such conflicts of interest, on the basis that these may still have an impact on staff's behaviour and participation in decision-making.

111. The policy should cover at least the following situations or relationships where conflicts of interest may arise:

a. economic interests (e.g. shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the institution to a company owned by staff, membership in a body or ownership of a body or entity with conflicting interests);

b. personal or professional relationships with the owners of qualifying holdings in the institution;

[46] This section should be read in conjunction with the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU, and the RTS on Confilcts of Interest for issuers of ARTs and CASPs under Regulation 2023/1114 EU.

c. personal or professional relationships with staff of the institution or entities included within the scope of prudential consolidation (e.g. family relationships);

d. other employment and previous employment within the recent past (e.g. five years);

e. personal or professional relationships with relevant external stakeholders (e.g. being associated with material suppliers, consultancies or other service providers); and

f. political influence or political relationships.

112. Notwithstanding the above, institutions should take into consideration that being a shareholder of an institution or having private accounts or loans with or using other services of an institution should not lead to a situation where staff are considered to have a conflict of interest if they stay within an appropriate de minimis threshold.

113. The policy should set out the processes for reporting and communication to the function responsible under the policy. Staff should have the duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest.

114. The policy should differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur unexpectedly with regard to a single event (e.g. a transaction, the selection of service provider, etc.) and can usually be managed with a one-off measure. In all circumstances, the interest of the institution should be central to the decisions taken.

115. The policy should set out procedures, measures, documentation elements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures. Such procedures, elements , responsibilities and measures should include:

a. entrusting conflicting activities or transactions to different persons;

b. preventing staff who are also active outside the institution from having inappropriate influence within the institution regarding those other activities;

c. establishing the responsibility of the members of the management body to abstain from voting on any matter where a member has or may have a conflict of interest or where the member's objectivity or ability to properly fulfil duties to the institution may be otherwise compromised;

d. preventing members of the management body from holding directorships in competing institutions, unless they are within institutions that belong to the same institutional protection scheme, as referred to in Article 113(7) of Regulation (EU) No 575/2013, credit institutions permanently affiliated to a central body, as referred

to in Article 10 of Regulation (EU) No 575/2013, or institutions within the scope of prudential consolidation.

116. The policy should specifically cover the risk of conflicts of interest at the level of the management body and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of members of the management body to take objective and impartial decisions that aim to fulfil the best interests of the institution. Institutions should take into consideration that conflicts of interest can have an impact on the independence of mind of members of the management body[47].

117. When mitigating identified conflicts of interests of members of the management body, institutions should document the measures taken, including the reasoning on how those are effective to ensure objective decision-making.

118. Actual or potential conflicts of interest that have been disclosed to the responsible function within the institution should be appropriately assessed and managed. If a conflict of interest of staff is identified, the institution should document the decision taken, in particular if the conflict of interest and the related risks have been accepted, and if it has been accepted, how this conflict of interest has been satisfactorily mitigated or remedied.

119. All actual and potential conflicts of interest at management body level, individually and collectively, should be adequately documented, communicated to the management body, and discussed, decided on and duly managed by the management body.

12.1 Conflict of interest policy in the context of loans and other transactions with members of the management body and their related parties

120. As part of their conflicts of interest policies for staff (Section 12) and the management of conflicts of interest of members of the management body as set out in Paragraph 117, the management body should set out a framework for identifying and managing conflicts of interest in the context of granting loans and entering into other transactions (e.g. factoring, leasing, property transactions, etc.) with members of the management body and their related parties.

121. Without prejudice to the national transposition of Directive 2013/36/EU[48], institutions may consider additional categories of related parties to whom they apply, in whole or in part, their conflicts of interest framework regarding loans and other transactions.

122. The conflicts of interest framework should ensure that decisions regarding the granting of loans and entering into other transactions with members of the management body and their

[47] See also the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.

[48] Please also refer to Basel Core Principle 20

related parties are taken objectively, without undue influence by conflicts of interests and are as a general principle conducted at arm's length.

123. The management body should set out the applicable decision-making processes for granting loans to and entering into other transactions with members of the management body and their related parties. This framework may provide for a differentiation between standard business transactions [49] entered into in the ordinary course of business and concluded on normal market terms and staff loans and transactions, which are concluded on conditions available to all staff. Furthermore, the conflicts of interest framework and decision-making process may differentiate between material and non-material loans and other transactions, different types of loans and other transactions and the level of actual or potential conflicts of interest they may create.

124. As part of the conflicts of interest framework, the management body should set appropriate thresholds (e.g. per product type, or depending on the conditions) above which the loan or other transaction with a member of the management body or its related parties always requires the approval by the management body. Decisions on material loans or other material transactions with members of the management body that are not being concluded under normal market terms, but on conditions available to all staff, should always be made by the management body.

125. The member of the management body benefitting from such a material loan or other material transaction or the member who is related to the counterparty, should not be involved in the decision-making.

126. When deciding on a loan or other transaction with a member of the management body or their related parties, before taking a decision, institutions should assess the risk to which the institution might be exposed due to the transaction.

127. Where loans are arranged as a line of credit (e.g. overdrafts), the initial decision and amendments thereof should be documented. Any use of such agreed credit facilities within the agreed limits should not be considered as a new decision on a loan to a member of the management body or their related party. Where an amendment of a line of credit is material in line with the institution's policy, a new assessment and decision should be made.

128. To ensure compliance with their conflict of interest policies, institutions should ensure that all relevant internal control procedures fully apply to loans and to other transactions with members of the management body or their related parties and that an appropriate oversight framework is in place at the level of the management body in its supervisory function.

[49] Business transactions include loans and other transactions (e.g. leasing, factoring, services in the context of initial public offerings (IPOs), mergers and acquisitions, selling and buying property).

12.2 Documentation of loans to members of the management body and their related parties and additional information

129. For the purpose of Article 88(1) of Directive 2013/36/EU, institutions should document data on loans[50] to members of the management body and their related parties properly, including at least:

a. the name of the debtor and their status (i.e. member of the management body or related party) and regarding loans to a related party, the member of the management body to whom the party is related and the nature of the relationship to the related party;

b. the type/nature of loan and the amount;

c. the terms and conditions applicable to the loan;

d. the date of approval of the loan;

e. the name of the individual or body and its composition taking the decision to approve the loan and the applicable conditions;

f. the fact (yes/no) as to whether or not the loan has been granted at market conditions; and

g. the fact (yes/no) as to whether or not the loan has been granted at conditions available to all staff.

130. Institutions should ensure that the documentation of all loans to members of the management body and their related parties is complete and updated and that the institution is able to make available to competent authorities the complete documentation in an appropriate format upon request without undue delay.

131. For a loan to a member of the management body or their related parties above an amount of EUR 200 000, institutions should be able to provide to the competent authority upon request the following additional information:

a. the percentage of the loan and the percentage of the sum of all outstanding amounts of loans towards the same debtor compared to:

i. the sum of its Tier 1 capital and Tier 2 capital and

ii. common equity Tier-1 capital of the institution;

b. whether the loan is part of a large exposure[51]; and

[50] See also EBA Guidelines on loan origination, available under: https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

[51] See also Part IV of Regulation (EU) No 575/2013 and in particular Article 392.

c. the relative weight of the aggregated sum of all outstanding amounts of loans towards the same debtor, calculated as a percentage by dividing the total outstanding amount by the total amount of all outstanding loans to members of the management body and their related parties.

13 Internal alert procedures

132. Institutions should put in place and maintain appropriate internal alert policies and procedures for staff to report potential or actual breaches of regulatory or internal requirements, including, but not limited to, those of Regulation (EU) No 575/2013 and national provisions transposing Directive 2013/36/EU, or of internal governance arrangements, through a specific, independent and autonomous channel. It should not be necessary for reporting staff to have evidence of a breach; however, they should have a sufficient level of certainty that provides sufficient reason to launch an investigation. Institutions should also implement appropriate processes and procedures that ensure that they comply with their obligations under the national implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

133. To avoid conflicts of interest, it should be possible for staff to report breaches outside regular reporting lines (e.g. through the compliance function, the internal audit function or an independent internal whistleblowing procedure). The alert procedures should ensure the protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679[52] (GDPR).

134. The alert procedures should be made available to all staff within an institution.

135. Information provided by staff through the alert procedures should, if appropriate, be made available to the management body and other responsible functions defined within the internal alert policy. Where required by the staff member reporting a breach, the information should be provided to the management body and other responsible functions in an anonymised way. Institutions may also provide for a whistleblowing process that allows information to be submitted in an anonymised way.

136. Institutions should ensure that the person reporting the breach is appropriately protected from any negative impact, e.g. retaliation, discrimination or other types of unfair treatment. The institution should ensure that no person under the institution's control engages in victimisation of a person who has reported a breach and should take appropriate measures against those responsible for any such victimisation.

137. Institutions should also protect persons who have been reported from any negative effects in case the investigation finds no evidence that justifies taking measures against that person. If measures are taken, the institution should take them in a way that aims to protect the

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

person concerned from unintended negative effects that go beyond the objective of the measure taken.

138. In particular, internal alert procedures should:

a. be documented (e.g. staff handbooks);

b. provide clear rules that ensure that information on the reporting and the reported persons and the breach are treated confidentially, in accordance with Regulation (EU) 2016/679, unless disclosure is required under national law in the context of further investigations or subsequent judicial proceedings;

c. protect staff who raise concerns from being victimised because they have disclosed reportable breaches;

d. ensure that the potential or actual breaches raised are assessed and escalated, including as appropriate to the relevant competent authority or law enforcement agency;

e. ensure, where possible, that confirmation of receipt of information is provided to staff who have raised potential or actual breaches;

f. ensure the tracking of the outcome of an investigation into a reported breach; and

g. ensure appropriate record keeping.

14 Reporting of breaches to competent authorities

139. Competent authorities should establish effective and reliable mechanisms to enable institutions' staff to report to competent authorities relevant potential or actual breaches of regulatory requirements, including, but not limited to, those of Regulation (EU) No 575/2013 and national provisions transposing Directive 2013/36/EU. These mechanisms should include at least:

a. specific procedures for the receipt of reports on breaches and follow-up, for instance a dedicated whistleblowing department, unit or function;

b. appropriate protection as referred to in Section 13;

c. protection of the personal data of both the natural person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679 (GDPR); and

d. clear procedures as set out in Section 13.

140. Without prejudice to the possibility of reporting breaches through the competent authorities' mechanisms, competent authorities may encourage staff to first try and seek to use their institutions' internal alert procedures.

Title V – Internal control framework and mechanisms

15 Internal control framework

141. Institutions should develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the institution and a robust and comprehensive internal control framework as referred to in Title V. Under this framework, institutions' business lines should be responsible for managing the risks they incur in conducting their activities and should have controls in place that aim to ensure compliance with internal and external requirements. ~~As part of this framework, institutions should have internal control functions with appropriate and sufficient authority, stature and access to the management body to fulfil their mission, and a risk management framework.~~

142. The internal control framework of institutions should be adapted on an individual basis to the specificity of its business, its complexity and the associated risks, taking into account the group context. Institutions should organise the exchange of the necessary information in a manner that ensures that each management body, business line and internal unit, including each internal control function, is able to carry out its duties. This means, for example, a necessary exchange of adequate information between the business lines and the compliance function and the AML/CFT compliance function where it is a separate control function, at the group level and between the heads of the internal control functions at the group level and the management body of the institution.

143. Institutions should implement appropriate processes and procedures that ensure that they comply with their obligations in the context of combating money laundering and terrorist financing. Institutions should assess their exposure to the risk that they may be used for the purpose of ML/TF and, where necessary, take mitigating measures to reduce those risks as well as their operational and reputational risks linked to them. Institutions should take measures to ensure that their staff is aware of such ML/TF risks and the impact that ML/TF has on the institution and the integrity of the financial system.

144. The internal control framework should cover the whole organisation, including the management body's responsibilities and tasks, and the activities of all business lines and internal units, including internal control functions, outsourced activities and distribution channels.

145. The internal control framework of an institution should ensure:

a. effective and efficient operations;

b. prudent conduct of business;

c. adequate identification, measurement and mitigation of risks;

d. the reliability of financial and non-financial information reported both internally and externally;

e. sound administrative and accounting procedures; and

f. compliance with laws, regulations, supervisory requirements and the institution's internal policies, processes, rules and decisions.

16 Implementing an internal control framework

146. The management body should be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework, processes and mechanisms, and for overseeing all business lines and internal units, including internal control functions (such as risk management, compliance, AML/CFT compliance, where separate from the compliance function, and internal audit functions). Institutions should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures, which should be approved by the management body.

147. An institution should have a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority within its internal control framework, including its business lines, internal units and internal control functions.

148. Institutions should communicate those policies, mechanisms and procedures to all staff and every time material changes have been made.

149. When implementing the internal control framework, institutions should establish adequate segregation of duties – e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons – and establish information barriers, e.g. through the physical separation of certain departments.

150. The internal control functions should verify that the policies, mechanisms and procedures set out in the internal control framework are correctly implemented in their respective areas of competence.

151. Internal control functions should regularly submit to the management body written reports on major identified deficiencies. These reports should include, for each new identified major deficiency, the relevant risks involved, an impact assessment, recommendations and corrective measures to be taken. The management body should follow up on the findings of the internal control functions in a timely and effective manner and require adequate remedial

actions. A formal follow-up procedure on findings and corrective measures taken should be put in place.

17 Risk management framework

152. As part of the overall internal control framework, institutions should have a holistic institution-wide risk management framework extending across all its business lines and internal units, including internal control functions, recognising fully the economic substance of all its risk exposures. The risk management framework should enable the institution to make fully informed decisions on risk-taking. The risk management framework should encompass on- and off-balance-sheet risks as well as actual risks and future risks that the institution may be exposed to. Risks should be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the institution and at consolidated or sub-consolidated level. All relevant risks should be encompassed in the risk management framework with appropriate consideration of ~~both~~ all categories of financial and non ~~-~~financial risks~~, including credit, market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance with AML/CTF and other financial crime and strategic risks.~~. The risk management framework should pay particular attention to ESG risks in the short and medium term and over a long-term horizon of at least 10 years, and to the channels through which they may drive their prudential risks, in particular through environmental physical and/or transition risks, and be compliant with the requirements set out in the EBA Guidelines on the management of ESG risks (EBA GL/2025/01).

153. An institution's risk management framework should include policies, procedures, risk limits and risk controls ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the risks at the business line, institution and consolidated or sub-consolidated levels.

154. An institution's risk management framework should provide specific guidance on the implementation of its strategies. This guidance should, where appropriate, establish and maintain internal limits consistent with the institution's risk appetite and commensurate with its sound operation, financial strength, capital base and strategic goals. An institution's risk profile should be kept within these established limits. The risk management framework should ensure that, whenever breaches of risk limits occur, there is a defined process to escalate and address them with an appropriate follow-up procedure.

155. The risk management framework should be subject to independent internal review, e.g. performed by the internal audit function, and reassessed regularly against the institution's risk appetite, taking into account information from the risk management function and, where established, the risk committee. Factors that should be considered include internal and external developments, including balance-sheet and revenue changes; any increase in the complexity of the institution's business, risk profile or operating structure; geographic expansion; mergers and acquisitions; and the introduction of new products or business lines.

156. When identifying and measuring or assessing risks, an institution should develop appropriate methodologies including both forward-looking and backward-looking tools. The methodologies should allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations. The tools should include the assessment of the actual risk profile against the institution's risk appetite, as well as the identification and assessment of potential and stressed risk exposures under a range of assumed adverse circumstances against the institution's risk capacity. The tools should provide information on any adjustment to the risk profile that may be required. Institutions should make appropriately conservative assumptions when building stressed scenarios.

157. Institutions should take into consideration that the results of quantitative assessment methodologies, including stress testing, are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). For example, models showing very high returns on economic capital may result from a weakness in the models (e.g. the exclusion of some relevant risks) rather than a superior strategy or excellent execution of a strategy on the part of the institution. The determination of the level of risk taken should not therefore be based only on quantitative information or model outputs; it should also comprise a qualitative approach (including expert judgement and critical analysis). Relevant macroeconomic environmental trends and data should be explicitly addressed to identify their potential impact on exposures and portfolios.

158. The ultimate responsibility for risk assessment lies solely with the institution, which, accordingly, should evaluate its risks critically and should not rely exclusively on external assessments. For example, an institution should validate a purchased risk model and calibrate it to its own individual circumstances to ensure that the model accurately and comprehensively captures and analyses the risk.

159. Institutions should be fully aware of the limitations of models and metrics and use not only quantitative but also qualitative risk assessment tools (including expert judgement and critical analysis).

160. In addition to the institutions' own assessments, institutions may use external risk assessments (including external credit ratings or externally purchased risk models). Institutions should be fully aware of the exact scope of such assessments and their limitations.

161. Regular and transparent reporting mechanisms should be established so that the management body, its risk committee, where established, and all relevant units in an institution are provided with reports in a timely, accurate, concise, understandable and meaningful manner and can share relevant information about the identification, measurement or assessment, monitoring and management of risks. The reporting framework should be well defined and documented.

162. Effective communication and awareness regarding risks and the risk strategy is crucial for the whole risk management process, including the review and decision-making processes, and helps prevent decisions that may unknowingly increase risk. Effective risk reporting involves sound internal consideration and communication of risk strategy and relevant risk data (e.g. exposures and key risk indicators), both horizontally across the institution and up and down the management chain.

18 New products and significant changes[53]

163. An institution should have in place a well-documented new product approval policy (NPAP), approved by the management body, that addresses the development of new markets, products and services, and significant changes to existing ones, as well as exceptional transactions. The policy should in addition encompass material changes to related processes (e.g. new ~~outsourcing~~third party arrangements) and ICT systems (e.g. ICT change processes). The NPAP should ensure that approved products and changes are consistent with the risk strategy and risk appetite of the institution and the corresponding limits of the institution, or that necessary revisions are made.

164. Material changes or exceptional transactions may include mergers and acquisitions, including the potential consequences of conducting insufficient due diligence that fails to identify post-merger risks and liabilities; setting up structures (e.g. new subsidiaries or single-purpose vehicles; new products; changes to systems or the risk management framework or procedures; and changes to the institution's organisation.

165. An institution should have specific procedures for assessing compliance with these policies, taking into account the input of the risk management function. This should include a systematic prior assessment and documented opinion by the compliance function for new products or significant changes to existing products.

166. An institution's NPAP should cover every consideration to be taken into account before deciding to enter new markets, deal in new products, launch a new service, or make significant changes to existing products or services. The NPAP should also include the definitions of 'new product/market/business' and 'significant changes' to be used in the organisation and the internal functions to be involved in the decision-making process.

167. The NPAP should set out the main issues to be addressed before a decision is made. These should include regulatory compliance; accounting; pricing models; the impact on risk profile, capital adequacy and profitability; the availability of adequate front, back and middle office resources; and the availability of adequate internal tools and expertise to understand and monitor the associated risks. Furthermore, to comply with obligations under Directive (EU) 2015/849, institutions should identify and assess the ML/TF risk associated with the new

[53] See also the EBA guidelines on product oversight and governance requirements for manufacturers and distributors of retail banking products, available at https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

product or business practice, and set out the measures to take to mitigate those risks. The decision to launch a new activity should clearly state the business unit and individuals responsible for it. A new activity should not be undertaken until adequate resources to understand and manage the associated risks are available.

168. The risk management function and the compliance function should be involved in approving new products or significant changes to existing products, processes and systems. Their input should include a full and objective assessment of risks arising from new activities under a variety of scenarios, of any potential shortcomings in the institution's risk management and internal control frameworks, and of the institution's ability to manage any new risks effectively. The risk management function should also have a clear overview of the roll-out of new products (or significant changes to existing products, processes and systems) across different business lines and portfolios, and the power to require that changes to existing products go through the formal NPAP process.

19 Internal control functions

169. In accordance with Article 76(5) of Directive 2013/36/EU, the internal control functions should include a risk management function (see Section 20), a compliance function (see Section 21) and an internal audit function (see Section 22). The risk management and compliance functions should also be subject to review by the internal audit function. The responsibilities of internal control functions also include ~~to ensure~~ensuring compliance with AML/CTF requirements.

170. The operational tasks of the internal control functions may be ~~outsourced~~performed by a third-party service provider, taking into account the proportionality criteria listed in Title I, to the consolidating institution or another entity within or outside of the group with the consent of the management bodies of the institutions concerned. Even when internal control operational tasks are partially or fully ~~outsourced~~provided by a third-party service provider, the head of the internal control function concerned and the management body are still responsible for these activities and for maintaining an internal control function within the institution.

171. ~~Without prejudice to national law implementing Directive 2015/849/EU~~In accordance with Regulation (EU) 2024/1624, institutions should assign the responsibility for ensuring the institution's compliance with the requirements of that ~~directive~~Regulation and the institution's policies and procedures to a ~~staff~~ member ~~(e.g. head of compliance). Institutions~~of the management body in its management function. Institutions may establish a separate AML/~~TF~~CFT compliance function as an independent control function.[54] The person responsible for the policies, procedures and controls in the day-to-day operation of the obliged entity's AML/~~CTF~~CFT requirements should, where necessary, be able to directly report to the management body ~~in its management and~~ its supervisory function.

[54] Please refer also to the EBA Guidelines on the AML/CTF compliance function (currently under development)

19.1 Heads of the internal control functions

172. The heads of internal control functions should be established at an adequate hierarchical level that provides the head of the control function with the appropriate authority and stature needed to fulfil ~~his or her~~their responsibilities. Notwithstanding the overall responsibility of the management body, in accordance with Article 76(6) of Directive 2013/36/EU, the heads of internal control functions should be independent ~~of the business lines or units they contro.~~ senior managers with distinct responsibility for the risk management, compliance and internal audit functions and be independent from the business lines or units they control. ~~To this end, the heads of the risk management, compliance and internal audit functions should report and be directly accountable to the management body, and theirperformance should be reviewed by the management body.~~ Where an internal control function is headed by a member of the management body in its management function, the institution should carefully ensure that appropriate safeguards and mitigants are in place to avoid conflicts of interest as referred to in paragraph 116, such as but not limited to, an independent mindset of the individual and appropriate key performance indicators, including objective appraisal and remuneration determination. This also applies to cases where the head of an internal control function performs other functions pursuant to section 19.3.

173. ~~Where necessary,~~ The heads of internal control functions should ~~be able to~~ have direct access and report directly to the management body in its supervisory function to raise concerns and warn the supervisory function, where appropriate, when specific developments affect or may affect the institution. This should not prevent the heads of internal control functions from reporting within the regular reporting lines as well. These arrangements should be reflected in the institution's mapping of duties and in the concerned persons' individual statements referred to in paragraphs 68a and 68b.

174. Institutions should have documented processes as referred to in article 68b in place to assign the position of the head of an internal control function and for withdrawing ~~his or her~~their responsibilities. In any case, the heads of internal control functions must not, under Article 76(6) of Directive 2013/36/EU be removed without the prior approval of the management body in its supervisory function. In significant institutions, competent authorities should be promptly informed about the approval and the main reasons for the removal of a head of an internal control function.

19.2 Independence of internal control functions

174a. In accordance with Article 76 paragraphs 5 and 6 of Directive 2013/36/EU, institutions should have internal control functions independent of the operational functions and of the members of the management body in its management function and of senior management, allowing them to have direct access and report directly, as appropriate, to the management body in its supervisory function.This independence should be achieved by having appropriate and sufficient authority and stature, the ability to access directly and escalate any issue to the management body in its supervisory function where appropriate to fulfil their mission.

175. In order for the internal control functions to be regarded as independent as per paragraph 174a, the following conditions should be met:

a. their staff do not perform any operational tasks that fall within the scope of the activities the internal control functions are intended to monitor and control;

b. they are organisationally separate from the activities they are assigned to monitor and control;

c. notwithstanding the overall responsibility of members of the management body for the institution, the head of an internal control function should not be subordinate to a person who has responsibility for managing the activities the internal control function monitors and controls; and

d. the remuneration of the internal control functions staff should not be linked to the performance of the activities the internal control function monitors and controls, and snot otherwise likely to compromise their objectivity[55]. The remuneration of the heads of internal control functions should be directly overseen by the management body in its supervisory function[56].

19.3 Combination of internal control functions

176. Taking into account the proportionality criteria set out in Title I, the risk management function and the compliance function may be combined under another senior person who may be a member of the management body in its management function as referred to paragraph 172, where the conditions in Article 76(6) 3rd subparagraph of Directive (EU) 2013/36 are met. In this case, institutions should be able to demonstrate that the nature, scale and complexity of the activities of the institution do not justify appointing a specific person for the risk management function or the compliance function, that the assessment of conflicts of interests required under Article 76 (6) 3rd subparagraph and as further specified in paragraph 172 has been performed, and, if necessary, measures to address identified conflicts of interest have been taken. The decision to combine the risk management function or the compliance function under another senior person should be documented. It should be ensured that the senior person fulfils the time commitment and suitability requirements laid out in Article 76(6) of Directive (EU) 2013/36. The internal audit function shouldmust not be combined with another internal control function.

19.4 Resources of internal control functions

[55] See also the EBA guidelines on sound remuneration policies, available at https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

[56] See also the EBA guidelines on sound remuneration policies, available at https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

177. Internal control functions should have sufficient resources. They should have an adequate number of qualified staff (both at parent level and at subsidiary level). Staff should remain qualified on an ongoing basis and should receive training as necessary.

178. Internal control functions should have appropriate ICT systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities. They should have access to all necessary information regarding all business lines and relevant risk-bearing subsidiaries, in particular those that can potentially generate material risks for the institutions.

20 Risk management function

179. Institutions should establish a risk management function (RMF) covering the whole institution. The RMF should have sufficient authority, stature and resources, taking into account the proportionality criteria listed in Title I, to implement risk policies and the risk management framework as set out in Section 17.

180. The RMF should have, where necessary, direct access to the management body in its supervisory function and its committees, where established, including in particular the risk committee.

181. The RMF should have access to all business lines and other internal units that have the potential to generate risk, as well as to relevant subsidiaries and affiliates.

182. Staff within the RMF should possess sufficient knowledge, skills and experience in relation to risk management techniques and procedures, and markets and products, and should have access to regular training.

183. ~~The RMF should be independent of the business lines and units whose risks it controls but should not be prevented from interacting with them.~~ Interaction between the operational functions and the RMF should help to achieve the objective of all the institution's staff bearing responsibility for managing risk.

184. The RMF should be a central organisational feature of the institution, structured so that it can implement risk policies and control the risk management framework. The RMF should play a key role in ensuring that the institution has effective risk management processes in place. The RMF should be actively involved in all material risk management decisions ~~.~~

185. Significant institutions may consider establishing dedicated RMFs for each material business line. However, there should be a central RMF, including a group RMF in the consolidating institution, to deliver an institution- and group-wide holistic view on all risks and to ensure that the risk strategy is complied with.

186. The RMF should provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by business lines or

internal units, and should inform the management body as to whether they are consistent with the institution's risk strategy and risk appetite. The RMF may recommend improvements to the risk management framework and corrective measures to remedy breaches of risk policies, procedures and limits.

20.1 RMF's role in risk strategy and decisions

187. The RMF should be actively involved at an early stage in elaborating the institution's risk strategy and in ensuring that the institution has effective risk management processes in place and should monitor the effective implementation of the risk strategy. The RMF should provide the management body with all relevant risk-related information to enable it to set the institution's risk appetite level. The RMF should assess the robustness and sustainability of the risk strategy and appetite. It should ensure that the risk appetite is appropriately translated into specific risk limits. The RMF should also assess the risk strategies and risk appetite of business units, including targets proposed by the business units, and should be involved before a decision is made by the management body concerning the risk strategies and risk appetite. Targets should be plausible and consistent with the institution's risk strategy. The RMF should provide the management body with all relevant information to establish ESG risk-related strategies, policies and plans with quantifiable targets, in line with the EBA guidelines on the management of ESG risks, particularly section 6.

188. The RMF's involvement in decision-making processes should ensure that risk considerations are taken into account appropriately. However, accountability for the decisions taken should remain with the business and internal units, and ultimately the management body. The business units should be involved in developing the quantifiable ESG risk-related targets referred to in the previous paragraph.

20.2 RMF's role in material changes

189. In line with Section 18, before decisions on material changes or exceptional transactions are taken, the RMF should be involved in the evaluation of the impact of such changes and exceptional transactions on the institution's and group's overall risk, and should report its findings directly to the management body before a decision is taken.

190. The RMF should evaluate how risks identified could affect the institution's or group's ability to manage its risk profile, its liquidity and its sound capital base under normal and adverse circumstances.

20.3 RMF's role in identifying, measuring, assessing, managing, mitigating, monitoring and reporting risks

191. The RMF should ensure that there is an appropriate risk management framework and that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the institution.

192. The RMF should ensure that identification and assessment are not based only on quantitative information or model outputs, but also take into account qualitative approaches. The RMF should keep the management body informed of the assumptions used in and potential shortcomings of the risk models and analysis.

193. The RMF should ensure that transactions with related parties are reviewed and that the risks they pose for the institution are identified and adequately assessed.

194. The RMF should ensure that all identified risks are effectively monitored by the business units.

195. The RMF should regularly monitor the actual risk profile of the institution and scrutinise it against the institution's strategic goals and risk appetite and ensure that ICT-related information is conveyed on a timely manner to enable decision-making by the management body in its management function and challenge by the management body in its supervisory function.

196. The RMF should analyse trends and recognise new or emerging risks and risk increases arising from changing circumstances and conditions. It should also regularly review actual risk outcomes against previous estimates (i.e. back testing) to assess and improve the accuracy and effectiveness of the risk management process.

197. The RMF should evaluate possible ways to mitigate risks. Reporting to the management body should include proposed appropriate risk-mitigating actions.

20.4 RMF's role in unapproved exposures

198. The RMF should independently assess breaches of risk appetite or limits (including ascertaining the cause and undertaking a legal and economic analysis of the actual cost of closing, reducing or hedging the exposure against the potential cost of keeping it). The RMF should inform the business units concerned and the management body, and recommend possible remedies. The RMF should report directly to the management body in its supervisory function when the breach is material, without prejudice for the RMF to report to other internal functions and committees.

199. The RMF should play a key role in ensuring a decision on its recommendation is made at the relevant level, complied with by the relevant business units and appropriately reported to the management body and, where established, the risk committee.

20.5 Head of the risk management function

200. The head of the RMF should be responsible for providing comprehensive and understandable information on risks and advising the management body, enabling this body to understand the institution's overall risk profile. The same applies to the head of the RMF of a parent institution regarding the consolidated situation.

201. The head of the RMF should ~~have~~be a senior manager with sufficient expertise, independence and seniority to challenge decisions that affect an institution's exposure to risks. ~~When the head of the RMF is not a member of the management body, significant institutions should appoint an independent head of the RMF who has no responsibilities for other functions and reports directly to the management body. Where it is not proportionate to appoint a person who is dedicated only to the role of head of the RMF, taking into account the principle of proportionality as set out in Title I, this function can be combined with the head of the compliance function or can be performed by another senior person, provided there is no conflict of interest between the functions combined. In any case, this person should have sufficient authority, stature and independence (e.g. head of legal).~~

202. The head of the RMF should be able to challenge decisions taken by the institution's management and its management body, and the grounds for objections should be formally documented. If an institution wishes to grant the head of the RMF the right to veto decisions (e.g. a credit or investment decision or the setting of a limit) made at levels below the management body, it should specify the scope of such a veto right, the escalation or appeal procedures, and how the management body will be involved.

203. Institutions should establish strengthened processes for the approval of decisions on which the head of the RMF has expressed a negative view. The management body in its supervisory function should be able to communicate directly with the head of the RMF on key risk issues, including developments that may be inconsistent with the institution's risk strategy and risk appetite.

21 Compliance function

204. Institutions should establish a permanent and effective compliance function to manage legal risk stemming from non-compliance ~~risk, and~~events. The compliance function should ~~appoint a person to~~ be headed by an independent senior manager responsible for this function across the entire institution (the compliance officer or head of compliance).

205. *deleted*

~~6. Where it is not proportionate to appoint a person who is dedicated only to the role of head of compliance, taking into account the principle of proportionality as set out in Title I, this function can be combined with the head of the RMF or can be performed by another senior person (e.g. head of legal), provided there is no conflict of interest between the functions combined.~~

206. *deleted*

~~7. The compliance function, including the head of compliance, should be independent of the business lines and internal units it controls and have sufficient authority, stature and resources. Taking into account the proportionality criteria set out in Title I, this function may~~

~~be assisted by the RMF or combined with the RMF or other appropriate functions, e.g. the legal division or human resources.~~

207. Staff within the compliance function should possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures, and should have access to regular training.

208. The management body in its supervisory function should oversee the implementation of a well-documented compliance policy, which should be communicated to all staff. Institutions should set up a process to regularly assess changes in the law and regulations applicable to its activities.

209. In accordance with Article 76(5) of Directive 2013/36, the compliance function assesses and mitigates legal risk stemming from non-compliance events and ensures that the institution's risk strategy and all material management decisions take into account legal risk stemming from non-compliance events. In particular, the compliance function should advise the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and should assess the possible impact of any changes in the legal or regulatory environment on the institution's activities and compliance framework.

210. The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that the compliance policy is observed. The compliance function should report to the management body and communicate as appropriate with the RMF on the institution's legal risk stemming from non-compliance ~~risk~~events and its management. The compliance function and the RMF should cooperate and exchange information as appropriate to perform their respective tasks. The findings of the compliance function should be taken into account by the management body and the RMF in decision-making processes.

211. In line with Section 18 of these guidelines, the compliance function should also verify, in close cooperation with the RMF and the legal unit, that new products and new procedures comply with the current legal framework and, where appropriate, with any known forthcoming changes to legislation, regulations and supervisory requirements.

212. Institutions should take appropriate action against internal or external behaviour that could facilitate or enable fraud, ML/TF or other financial crime and breaches of discipline (e.g. breaches of internal procedures, breaches of limits).

213. Institutions should ensure that their subsidiaries and branches take steps to ensure that their operations are compliant with local laws and regulations. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches should inform the compliance officer or the head of compliance of the consolidating institution.

22 Internal audit function

214. Institutions should set up an independent and effective internal audit function (IAF), taking into account the proportionality criteria set out in Title I, and should appoint a person to be responsible for this function across the entire institution. The IAF should be independent and have sufficient authority, stature and resources. In particular, the institution should ensure that the qualification of the IAF's staff members and the IAF's resources, in particular its auditing tools and risk analysis methods, are adequate for the institution's size and locations, and the nature, scale and complexity of the risks associated with the institution's business model, activities, risk culture and risk appetite.

215. The IAF should be independent of the audited activities. ~~Therefore, the IAF should not be combined with other functions.~~

216. The IAF should, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of an institution, including outsourced activities, with the institution's policies and procedures and with regulatory requirements. Each entity within the group should fall within the scope of the IAF.

217. The IAF should not be involved in designing, selecting, establishing and implementing specific internal control policies, mechanisms and procedures, and risk limits. However, this should not prevent the management body in its management function from requesting input from internal audit on matters related to risk, internal controls and compliance with applicable rules.

218. ~~The IAF should~~The IAF should perform an independent review of the effective implementation of the institution's risk strategy and assess whether the institution's internal control framework as set out in Section 15 is both effective and efficient. In particular, the IAF should assess:

a. the appropriateness of the institution's governance framework;

b. whether existing policies and procedures remain adequate and comply with legal and regulatory requirements and with the risk strategy and risk appetite of the institution;

c. the compliance of the procedures with the applicable laws and regulations and with decisions of the management body;

d. whether the procedures are correctly and effectively implemented (e.g. compliance of transactions, the level of risk effectively incurred, etc.); and

e. the adequacy, quality and effectiveness of the controls performed and the reporting done by the defence business units and the risk management and compliance functions.

219. The IAF should verify, in particular, the integrity of the processes ensuring the reliability of the institution's methods and techniques, and the assumptions and sources of information used in its internal models (e.g. risk modelling and accounting measurements). It should also evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken.

220. The IAF should have unfettered institution-wide access to all the records, documents, information and buildings of the institution. This should include access to management information systems and minutes of all committees and decision-making bodies.

221. The IAF should adhere to national and international professional standards. An example of the professional standards referred to here is the global internal audit standards established by the Institute of Internal Auditors.

222. Internal audit work should be performed in accordance with an audit plan and a detailed audit programme following a risk-based approach.

223. An internal audit plan should be drawn up at least once a year on the basis of the annual internal audit control objectives. The internal audit plan should be approved by the management body.

224. All audit recommendations should be subject to a formal follow-up procedure by the appropriate levels of management to ensure and report on their effective and timely resolution.

Title VI – Business continuity management[57]

225. Institutions should establish a sound business continuity management, encompassing appropriate planning and ~~recovery plan~~testing to ensure their ability to operate on an ongoing basis and to limit losses in the event of severe business disruption. This should encompass the institution's business continuity policy and response and recovery plans. Moreover, with respect to the management of ICT risks, the business continuity management should be consistent with the DORA framework[58], in particular the ICT business continuity policy adopted according to Article 11 (1) of Regulation (EU) 2022/2554.

226. Institutions may establish a specific independent business continuity function, e.g. as part of the RMF. The ICT crisis management function established pursuant to Article 11(7) of Regulation (EU)2022/2554 may be a part of this function.

227. *deleted*

[57] ~~Institutions should also refer to the EBA Guidelines on ICT risk:, available under: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management~~

[58] In particular Articles 5(2)e, 11 of Regulation (EU) 2022/2554 (DORA) as well as Articles 24 to 26 of Commission Delegated Regulation (EU) 2024/1774.

~~An institution's business relies on several critical resources (e.g. IT systems, including cloud services, communication systems, core staff and buildings). The purpose of business continuity management is to reduce the operational, financial, legal, reputational and other material consequences arising from a disaster or extended interruption to these resources and consequent disruption to the institution's ordinary business procedures. Other risk management measures might be intended to reduce the probability of such incidents or to transfer their financial impact to third parties (e.g. through insurance).~~

228. In order to establish a sound business continuity management ~~plan~~, an institution should ~~carefully analyse risk factors for and its exposure to severe business disruptions and assess~~perform a business impact analysis to identify and measure (quantitatively and qualitatively) the~~ir~~ potential impact of severe business disruptions, using internal and~~/or~~ external data and scenario analysis. This analysis should cover all business lines and internal units, including the RMF, and should take into account ~~their interdependency.~~key interdependencies. The results of the analysis should contribute to defining the institution's recovery priorities and objectives.

229. On the basis of the abovementioned analysis, an institution should put in place:

a. ~~contingency and~~ business continuity and contingency plans to ensure ~~that~~ the institution ~~reacts~~would be able to react appropriately to ~~emergencies~~disruptions and ~~is able~~ to maintain its ~~most~~critical or important ~~business activities if there is~~functions in case of disruption ~~to its ordinary business procedures~~; and

b. response and recovery plans for critical ~~resources~~or important functions to enable the institution to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions should be consistent with the institution's risk appetite.

230. ~~Contingency,~~ Business continuity, contingency, response and recovery plans should be documented and carefully implemented~~.~~ and subject to internal audit review. The documentation should be available ~~within~~to the ~~business lines, internal units and RMF~~staff involved in the execution of the plans, and should be stored on systems that are physically separated and readily accessible in case of ~~contingency~~emergency. Appropriate operational resilience and business continuity awareness, including training, should be provided. Plans should be regularly tested and updated. ~~Any challenges or failures occurring in the tests~~Testing results should be documented ~~and~~, analysed, ~~with~~reported to the management body and be used to review the plans ~~reviewed~~ accordingly.

Title VII – Transparency

231. Strategies, policies and procedures should be communicated to all relevant staff throughout an institution. An institution's staff should understand and adhere to policies and procedures pertaining to their duties and responsibilities.

232. Accordingly, the management body should inform and update the relevant staff about the institution's strategies and policies in a clear and consistent way, at least to the level needed to carry out their particular duties. This may be done through written guidelines, manuals or other means.

233. Where parent undertakings are required by competent authorities under Article 106(2) of Directive 2013/36/EU to publish annually a description of their legal structure and governance and the organisational structure of the group of institutions, the information should include all entities within the group structure as defined in Directive 2013/34/EU[59], by country.

234. The publication should include at least:

a. an overview of the internal organisation of the institutions and the group structure as defined in Directive 2013/34/EU and changes thereto, including the main reporting lines and responsibilities;

b. any material changes since the previous publication and the date of the material change;

c. new legal, governance or organisational structures;

d. information on the structure, organisation and members of the management body, including the number of its members and the number of those qualified as independent, and specifying the gender and duration of the mandate of each member of the management body;

e. the key responsibilities of the management body;

f. a list of the committees of the management body in its supervisory function and their composition;

g. an overview of the conflict of interest policy applicable to the institution and to the management body;

h. an overview of the internal control framework; and

i. an overview of the business continuity management framework.

[59] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

Annex I – Aspects to take into account when developing an internal governance policy

In line with Title III, institutions should consider the following aspects when documenting internal governance policies and arrangements:

1. Shareholder structure
2. Group structure, if applicable (legal and functional structure)
3. Composition and functioning of the management body
   a) selection criteria, including how diversity is taken into account
   b) number, length of mandate, rotation, age
   c) independent members of the management body
   d) executive members of the management body
   e) non-executive members of the management body
   f) internal division of tasks, if applicable
4. Governance structure and organisation chart (with impact on the group, if applicable)
   a) specialised committees
      i. composition
      ii. functioning
   b) executive committee, if any
      i. composition
      ii. functioning
5. Key function holders
   a) head of the risk management function
   b) head of the compliance function
   c) head of the internal audit function
   d) chief financial officer
   e) other key function holders
6. Internal control framework
   a) description of each function, including its organisation, resources, stature and authority

7. Description of the risk strategy and risk management framework and how ESG risks ~~and risk factors~~ are taken into account
8. Organisational structure (with impact on the group, if applicable)
    a) operational structure, business lines, and allocation of competences and responsibilities
    b) outsourcing
    c) range of products and services
    d) geographical scope of business
    e) provision of services under the regime of freedom of provision of services
    f) branches
    g) subsidiaries, joint ventures, etc.
    h) use of offshore centres
9. Code of conduct and behaviour (with impact on the group, if applicable)
    a) strategic objectives and company values
    b) internal codes and regulations, prevention policy
    c) conflict of interest policy
    d) whistleblowing
10. Status of the internal governance policy, with date
    a) development
    b) last amendment
    c) last assessment
    d) approval by the management body.

Annex II – Optional template for individual statements of roles and duties

1. Personal identification details

Name of the institution:

Date from which this statement is in effect and has been updated :DD/MM/YYYY

Position:

Family name	
First name	
Other names used by the person (including birth name where available)	

Date of birth	
Place of birth (country + city)	
Contact phone number	
Email	

In case of a risk of confusion due to the presence of several persons bearing the same name within institution, please provide further identification details (e.g. previous position) :

2. Individual roles and duties fulfilled

Please fill in all required fields according to the following instructions:

- In the Roles Table, please indicate the level ('member of the management body in its management function' or 'senior manager' or 'key function holder'[60]) and description of the role(s) performed by the individual, leveraging to the extent possible on examples provided, with the possibility to deviate from the list where other arrangements are in place, and any other relevant and necessary information pertaining to the role(s).
- In the **Duties Tabl**e, please list all the relevant and applicable duties the individual is expected to perform within their role(s), including the effective starting date from which they are carrying out each duty and whether that is shared with other roles.

[60]The applicable definitions of 'management body', 'senior management' and 'key function holder' are those of Article 3 of Directive 2013/36/EU. For the purposes of this statement, if the individual is a key function holder who is also a senior manager, please indicate 'senior manager'. If the individual is a key function holder who is not a senior manager, please indicate 'key function holder'.

- Column A: please indicate a number for each duty, adding rows if necessary;
- Column B: please describe the duty;
- Column C: please include the effective date from which this person has the duty;

- Column D: where duties are shared (for example, as part of a job share or of a handover of duties), please provide details of any sharing arrangements, including the name and position of the individual(s) the duty is shared with, and explain which components each person is responsible for. The duty should be recorded in the same way in the statements for each individual involved in the shared duty.

Roles Table

Level of the position	*Please indicate 'member of the management body in its management function' or 'senior manager' or 'key function holder'*
Role(s) Description	*Please list here all the role(s) the individual fulfils, for example (not limited to):* *Chair of MBMF, Member of MBMF other than chair, Chief executive officer, Chief financial officer, Chief operating officer, Chief risk officer, Chief compliance officer, Head of internal audit, Head of AML, etc.*
Time commitment	*Please detail the expected time commitment for this role (e.g. 100%, 30 hours per week etc)*
Additional information	

Duties Table

(A) #	**(B) Duty**	**(C) Effective date**	**(D) Details if shared duty**
		DD/MM/YYYY	
Additional information			

5. Accompanying documents

5.1. Draft cost-benefit analysis/impact assessment

1. Article 16(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) (EBA Regulation) provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any guidelines it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

A. Problem identification and policy objectives

2. Directive 2013/36/EU has been amended in 2021, following the Directive 2019/878/EU. It is being amended again following the amendments in Directive (EU)2024/1619. The EBA Guidelines on internal governance needed to be amended to reflect those changes and to align their wording with other EBA work.
3. The 2021 amendments to the guidelines ensure that institutions have specific governance arrangements regarding the management of money laundering and terrorist financing risks and to avoid that they contribute to dividend arbitrage schemes. Institutions should also have a strong framework to manage conflicts of interests and ensure prudent decision-making in the context of loans to related parties.
4. The 2025 amendments to the guidelines ensure the guidelines:

    - specify further the requirements introduced by the newly introduced Article 48g of Directive (EU) 2013/36 on third country branches' sound internal governance arrangements taking into account third country branches specificities,

    - should ensure that institutions draw up, maintain and update individual statements setting out the roles and duties of all members of the management body in its management function, of senior management and of key function holders and a mapping of duties, according to Article 88 (3) of Directive (EU) 2013/36.

B. Baseline scenario

5. The current EU legislative framework for institutions' internal governance consists mainly of Directive 2013/36/EU and its subsequent amendments, the EBA guidelines on internal governance, the EBA Guidelines on the assessment of the suitability of members of the management body and key function holders and the EBA Guidelines on third-party risk

management (formerly Guidelines on outsourcing), and EBA Guidelines on management of ESG risks.

6. The impact assessment covers guidelines developed to ensure the harmonised application of additional governance requirements introduced by Directive 2013/36/EU and areas where the policy has changed. Areas that have not changed in substance and the underlying changes introduced by the Directive 2013/36/EU and Regulation (EU) No 575/2013 have not been assessed.

C. Options considered

2021 amendments

7. Guidelines have been provided on the code of conduct that link the guidelines to the requirements on non-discrimination and equal opportunities within the European Charter of Fundamental Rights and the Treaty on the Functioning of the European Union. Those additions have no impact as the underlying provisions are fundamental principles that are already implemented by Member States based on the aforementioned frameworks. The EBA has to take those frameworks into account when setting out guidelines.

8. The guidelines provide additional clarity about the institutions internal governance in the context of AML/CTF provisions. Institutions should already have sufficient governance arrangements in place to ensure that they comply with Anti-Money Laundering, Anti-Terrorist Financing and tax laws. The related risks are already covered by the CRD requirement on institutions to manage all their risks. Hence, the clarifications provided in the guidelines should not trigger any implementation costs if the institution concerned already had the required arrangements in place and had implemented the requirements under Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015.

9. In addition the guidelines have been clarified regarding the management of conflicts of interest in relation to loans and other transactions to members of the management body and their related parties. Given that specific provisions have been added to Directive 2013/36/EU it was considered necessary to clarify the regulatory expectations and the requirements with regard to the documentation of such loans and the management of related conflicts of interest. It is necessary that institutions document all loans and transactions. The specific documentation elements on such loans in the guidelines are limited and do not create a material burden. The need to identify such loans, to document them and to comply with the GDPR in this context is created by the requirement within the Capital Requirements Directive (CRD). Hence, the costs for those aspects are not assessed as part of this impact assessment.

10. The objective of the changes are that there is sufficient scrutiny on decisions regarding such loans and that conflicts of interest in that context are appropriately managed. Restricting the guidelines to loans to members of the management body and their related parties would not be effective as other transactions might also create material conflicts of interests. Limited additional documentation elements regarding the conditions of such loans as compared to

market conditions and their volumes are necessary to assess the appropriateness of the management of conflicts of interests. Given the need to document contractual conditions and to comply e.g. with the large loan regime it is assessed that the additional costs for providing the additional information, when requested, is low.

11. In line with the principle of proportionality, the guidelines differentiate between material and non-material loans and transactions. The guidelines further specify the already existing CRD requirements for all institutions.

2025 amendments

12. Directive 2024/1619 introduces amendments to Directive 2013/36/EU to ensure that third country branches meet internal governance and risk control requirements. These requirements represent one part of a harmonised framework for TCBs within the EU which was introduced due to their material footprint in EU banking markets and therefore risks to the financial stability in the EU, as well as due to the currently scattered prudential and supervisory requirements that they are subject to. While these requirements are new, TCBs were expected also in the past to fulfil a minimum standard in terms of internal governance for supervisory purposes, while part of these requirements were also reflected in the EBA Opinion on the set-up and operationalisation of Intermediate EU Parent Undertaking(s) under Article 21b CRD[61]. Finally, given that the new requirements for TCBs are envisaged in the Directive, the costs of these additional clarifications provided by the Guidelines are expected to be minor.

13. The amendments include new requirements for institutions to draw up, maintain and update individual statements setting out the roles and duties of all members of the management body in its management function, of senior management and of key function holders. The guidelines provide additional details on the way these individual statements are to be elaborated, with an optional template included in the Annex. The option of no template and mandatory template were considered, but both were discarded to ensure that institutions are provided as much as possible guidance, while limiting the potential constraints associated with a fixed template that may not fully reflect their governance structure. Given that the individual statements is a requirement of the Directive, and that the templates are optional, the costs of these additional clarifications provided by the Guidelines are expected to be small.

14. In a similar manner, institutions should also draw up, maintain and update a mapping of duties, including details of the reporting lines, of the lines of responsibility, and of the persons who are part of the governance arrangements. Given the high dependence of the mapping of duties on the individual structures of the institutions, no template was considered for this requirement. The approach is principle-based, and the institutions are provided the flexibility to present the mapping of duties in the way they see fit, as long as the general principles are

[61] https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20on%20the%20set-up%20and%20operationalisation%20of%20IPUs%20%28EBA-Op-2022-12%29/1042791/Opinion%20on%20the%20set-up%20and%20operationalisation%20of%20IPUs.pdf

followed. Given that the mapping of duties is a requirement of the Directive, the costs of these additional clarifications provided by the Guidelines are expected to be negligible.

15. The guidelines also required redrafting in certain areas to reflect the results of the EBA benchmarking report of diversity practices and gender-neutral remuneration policies, the consideration of ESG risks in the short, medium and long term in prudential framework according to Article 87a of the Directive (EU) 2013/36 and the EBA Guidelines on management of ESG risks, the changes brought by the entry into force of the digital operational resilience framework under Directive (EU) 2022/2554 related to the management of ICT risk and the ICT risk management function. These changes do not entail any significant costs of implementation, as they mostly ensure an allignement of wording and references with new or updated legislative documents.

D. Cost-benefit analysis

16. With respect to the 2021 amendments, given the limited amendments to the guidelines and given that they are based on amendments of Directive 2013/36/EU and other existing legal requirements, it is assumed that changes to the guidelines create no or very low implementation costs for updates to internal policies and additional documentation.

17. With respect to the 2025 amendments, given the limited amendments to the guidelines and given that they are based on amendments of Directive 2013/36/EU and other existing legal requirements, the changes to the guidelines create no or low implementation costs related to the clarifications on the requirements for TCBs to meet internal governance and risk control requirements, and for institutions to produce and maintain individual statements according to an optional harmonised template.

5.2 Questions for public consultation

Question 1: Are subject matter, scope of application, definitions and date of application appropriate and sufficiently clear?

Question 2: Are the changes made in Titles I (proportionality) and II (role of the manamgnet body and committees) appropriate and sufficiently clear?

Question 3: Are the changes made in Title III (governance framework) section 6 appropriate and sufficiently clear?

Question 4: Are the changes made in Title III section 7 (third-country branches) appropriate and sufficiently clear?

Question 5: Are the changes made in Title IV (risk culture) appropriate and sufficiently clear?

Question 6: Are the changes made in Title V (internal control framework) appropriate and sufficiently clear?

Question 7: Are the changes made in Title VI (business continuity managment) appropriate and sufficiently clear?