EBA/GL/2026/10

5 November 2026

# Final report on

## Guidelines

## on internal governance under Directive 2013/36/EU

# Table of content

**Executive summary** 4

**Background and rationale** 5

**Guidelines on internal governance under Directive 2013/36/EU** 14

**1. Compliance and reporting obligations** 15

**2. Subject matter, scope and definitions** 16

**3. Implementation** 19

**4. Guidelines** 20

Title I – Proportionality 20

Title II – Role and composition of the management body and committees 21

1 Role and responsibilities of the management body 21

2 Management function of the management body 24

3 Supervisory function of the management body 25

4 Role of the chair of the management body 26

5 Committees of the management body in its supervisory function 26

5.1 Setting up committees 26

5.2 Composition of committees 27

5.3 Committees' processes 29

5.4 Role of the risk committee 29

5.5 Role of the audit committee 31

5.6 Combined committees 32

Title III – Governance framework 32

6 Organisational framework and structure 32

6.1 Organisational framework 32

6.2 Know your structure 34

6.3 Complex structures and non-standard or non-transparent activities 35

7 Organisational framework 37

7.1 Application in a group context 37

7.2 Third-country branches' internal governance arrangements 38

Title IV – Risk culture and business conduct 41

8 Risk culture 41

9 Corporate values and code of conduct 42

10 Conflict of interest policy at institutional level 44

11 Conflict of interest policy for staff 45

11.1 Conflict of interest policy in the context of loans and other transactions with members of the management body and their related parties 47

11.2 Documentation of loans to members of the management body and their related parties and additional information 49
12 Internal alert procedures 50
13 Reporting of breaches to competent authorities 51
Title V – Internal control framework and mechanisms 52
14 Internal control framework 52
15 Implementing an internal control framework 53
16 Risk management framework 54
17 New products and significant changes 56
18 Internal control functions 57
18.1 Heads of the internal control functions 58
18.2 Independence of internal control functions 58
18.3 Combination of internal control functions 59
18.4 Resources of internal control functions 59
19 Risk management function 60
19.1 RMF's role in risk strategy and decisions 60
19.2 RMF's role in material changes 61
19.3 RMF's role in identifying, measuring, assessing, managing, mitigating, monitoring and reporting risks 61
19.4 RMF's role in unapproved exposures 62
19.5 Head of the risk management function 62
20 Compliance function 63
21 Internal audit function 64
Title VI – Business continuity management 65
Title VII – Transparency 66
**Annex – Optional template for individual statements of roles and duties 68**
**5. Accompanying documents 70**
5.1. Draft cost-benefit analysis/impact assessment 70
5.2. Views of the Banking Stakeholder Group (BSG) 74
5.3. Feedback on the public consultation and on the opinion of the Banking Stakeholder Group (BSG) 75

# Executive summary

Confidence in the reliability of the financial system is essential for its proper functioning and its contribution to the economy. Effective internal governance arrangements are a key prerequisite for the safe and prudent management of institutions and for financial stability. Robust governance is a key requisite for the financial sector's resilience and ensures that sound financial services are provided to the economy. To further harmonise institutions' internal governance arrangements, processes and mechanisms within the Union, the European Banking Authority (EBA) is mandated, under Article 74(3) of Directive 2013/36/EU, to develop guidelines in this area. The Guidelines apply to all institutions, irrespective of their governance structures (including unitary, dual or other models), without advocating or favouring any particular structure.

The EBA Guidelines on internal governance were initially developed to address governance weaknesses identified in the aftermath of the global financial crisis notably with regard to the role and oversight of management bodies, the effectiveness of internal control functions, risk culture and accountability, and to promote a consistent supervisory approach across Member States. Since their initial publication, internal governance has continued to receive increased supervisory and regulatory attention, reflecting the growing complexity of institutions' activities and risk profiles. Supervisory focus has expanded to new and emerging risks, including conduct-related risks, such as deficiencies in AML/CFT frameworks, the integration of environmental, social and governance (ESG) considerations, and the impact of digitalisation, innovation, artificial intelligence and increased interconnectedness. These developments have increased institutions' exposure to ICT-related risks and dependencies on third-party service providers and new technologies.

The Guidelines have been amended to reflect these developments and the changes introduced by the revised Union legal framework. In particular, the amendments ensure alignment with Directive (EU) 2024/1619 (CRD VI), Directive (EU) 2019/878 and Regulation (EU) 2022/2554 (DORA) and the related RTS, ITS and Guidelines. The guidelines on internal governance clarify further the responsibilities of the management body and the mapping of roles and duties of members of the management body, senior management and key function holders. The Guidelines also specify the governance requirements for third-country branches, taking into account their specificities.

The revised Guidelines should be applied taking into account the principle of proportionality, ensuring that governance arrangements are commensurate with institutions' size, complexity, risk profile and business model, and remain consistent with relevant international standards. The amendments aim to ensure that the Guidelines remain relevant and effective, support consistent supervisory practices across the Union, and contribute to the resilience and sound functioning of the EU financial system.

# Background and rationale

1. Trust in the reliability of the financial system is crucial for its proper functioning and is a prerequisite for its contribution to the broader economy. Robust governance is a key requisite for the financial sector's resilience and ensures that sound financial services are provided to the economy. Consequently, effective internal governance arrangements are fundamental if institutions, individually and the banking system they form, are to operate well.

2. Over recent years, internal governance has continued to receive enhanced supervisory and regulatory attention at international, Union and national level, reflecting its central role in ensuring sound management, financial stability and the protection of depositors and other stakeholders. While earlier initiatives primarily sought to address weaknesses identified during the global financial crisis of 2008 and subsequent supervisory reviews, more recent developments have expanded the scope of supervisory focus.

3. In particular, supervisory focus has further expanded to conduct-related risks and deficiencies, including shortcomings in anti-money laundering and counter‑terrorist financing (AML/CFT), governance weaknesses related to activities involving offshore financial centres, and the integration of ESG factors into institutions' business strategies, risk management frameworks and internal controls. At the same time, increased innovation, digitalisation and increased interconnectedness within the financial system have significantly increased institutions' exposure to ICT-related risks, including cyber risk and data-related vulnerabilities.

4. These developments have materially increased the complexity of institutions' activities and business models. The use of advanced technologies, including, cloud services, artificial intelligence and quantum technologies, has amplified the likelihood and potential impact of ICT‑related incidents, including severe but plausible operational disruptions. In parallel, the growing relevance of sustainability considerations requires institutions to adequately identify, assess and manage ESG‑related risks. Furthermore, the expansion of cross‑border activities, including through third‑country branches, has reinforced the need for effective governance oversight and clear accountability to ensure compliance with Union requirements and to mitigate risks of regulatory arbitrage.

5. Operational resilience, understood as the ability of institutions to ensure the continuity of critical operations in the event of disruption, is an integral part of the sound governance arrangements and effective internal control mechanisms required pursuant to Article 74 of Directive 2013/36/EU (CRD).

6. Strong internal governance arrangements are essential to ensure effective oversight by the management body, to promote a sound and consistent risk culture, and support a robust, integrated internal control framework at all levels of the institution and, where applicable, at group level. Strong governance arrangements are also essential to enable competent

authorities to monitor, on a risk‐based basis, the adequacy and effectiveness of institutions' governance frameworks.

7. The guidelines should be applied taking into account the principle of proportionality, recognising that governance arrangements should be tailored to institution's size, complexity, risk profile, and business model. While significant institutions are expected to implement more sophisticated governance frameworks, smaller and less complex institutions may adopt simpler arrangements, provided they remain effective and prudent. These guidelines are also consistent with international standards published by the Basel Committee on Banking Supervision (BCBS) and the Financial Stability Board (FSB).

8. The Guidelines have also been amended to specify further the requirements introduced by Article 48g of Directive (EU) 2013/36/EU as amended by Directive (EU) 2024/1619 on third country branches' sound internal governance arrangements taking into account third country branches specificities as well as to ensure consistency with the DORA framework.

## 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 [1] in application of Article1(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.

[1] 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

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 current and future impacts of ESG factors including through specific plans, quantifiable targets and processes to address them[2], 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 guidelines refer, regarding the second line of defence, to the 'risk management function' and '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

[2] 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.

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 undertakings that are not themselves subject to this directive have to 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[3].

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 to identify, measure, monitor and control transactions with their parent mixed-activity holding company and its subsidiaries appropriately.

18. Where Article 48g 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. 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, who should be of sufficiently good repute and possess sufficient knowledge, skills and experience and commit sufficient time to the performance of their duties[4]. 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 functions independent from the operational functions. Third-country branches should establish sound remuneration policies, 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. Third-country branches and subsidiaries within the EU cannot be empty shells that do not have the sufficient substance to be authorised.

19. Article 48g(3) of Directive 2013/36/EU provides that Class 2 third country branches (TCBs) are required to comply with Article 76(5) and with the first, second and fourth subparagraphs of Article 76(6), implying that they should have effective internal control functions without necessarily distinguishing between the risk management and compliance functions, and

[3] See EBA guidelines on sound remuneration policies.

[4] 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

without requiring prior approval by the management body in its supervisory function for the removal of the heads of those functions. However, considering the application of the principle of proportionality, competent authorities may require Class 2 TCBs, having regard to their size, complexity and risk profile, to apply additional elements of Article 76(6), namely subparagraphs three and five, including the separation of the risk management and compliance functions and the requirements relating to the appointment and removal of the heads of internal control functions.

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 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) including the use of frontier AI and quantum technologies, 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, institutions should take into account ESG factors within their risk management framework, in line with the requirements set out by the EBA guidelines on the management of ESG risks[5].

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

24. In addition, it is necessary to take into account the entry into force of the digital operational resilience framework under Regulation (EU) 2022/2554[6] 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 defence model taking into account the application of the principle of proportionality. The requirements introduced by Regulation (EU) 2024/1689[7] on providing artificial intelligence systems and the risks of fundamental rights violation and discrimination have been also taken into account. 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)[8]; 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.

25. 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.

26. 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.

27. In Member States where the management body delegates, partially or fully, the executive function to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons who perform those executive functions and direct the business of the institution on the basis of that delegation should be understood as constituting the management function of the management body as defined under Directive 2013/36/EU. 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. For the purposes of these guidelines, any reference to the management body in its management function should be understood as including also the members of the

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

[7] 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)

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

executive body or the CEO, as defined 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.

28. 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 of the management body, and provides appropriate advice. The oversight roles include reviewing the performance of the management function of the management body and the achievement of objectives, constructively 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.

29. 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.

30. Independent directors within the supervisory function of the management body help 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[9].

31. 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.

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

33. 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 regulatory requirements.

[9] 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.

34. 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 and risk management functions 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.

35. The risk management and compliance functions 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 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 implemented by the first line of defence are properly designed and effective. The compliance function monitors compliance with legal and regulatory requirements and internal policies, provides advice on compliance to the management body and other relevant staff, and establishes policies and processes to manage compliance risk stemming from non-compliance events. Both functions may intervene to ensure the modification of internal control and risk management systems within the first line of defence where necessary.

36. 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 control functions, units and business lines. The internal audit function performs its tasks independently from the other lines of defence.

37. 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, should have direct access and can report directly to the management body in its supervisory function. Internal control functions should be able 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.

38. 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 also depend on the classification of third-country branches as class 1 or class 2.

39. 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.

40. 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 and compliance functions 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 regulatory requirements.

41. 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.

42. 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 exists. The institution, its organisational substructures, staff and shareholders hold different interests that should be considered in such a framework 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.

43. 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/GL/2026/10

5 November 2026

# Guidelines on internal governance under Directive 2013/36/EU

# 1. Compliance and reporting obligations

## Status of these guidelines

1. These guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010[10]. 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/2026/10'. 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.

[10] 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 including branches of credit institutions having their head undertaking in a third country that are subject to Directive 2013/36/EU[11] 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

6. 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 including central bodies as referred to in Article 10 of Regulation (EU) No 575/2013 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. These Guidelines are also addressed to third-country branches (TCBs) 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 (all the above referred to as 'institutions'; TCBs only for the purpose of the limited scope outlined in paragraph 12).

## Scope of application

7. 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[12] they are or might be exposed to, their network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554 and their internal control framework.

8. 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

[11] 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).

[12] Any reference to risks in these guidelines should include also money laundering and terrorist financing risks as well as environmental, social and governance risks, and risks in the context of the use of artificial intelligence and quantum technologies.

irrespective of the board structure used (unitary and/or a dual board structure and/or another structure) across Member States. The management body, as defined in Article 3(1)(7) of Directive 2013/36/EU should be understood as having management (executive) in accordance with Article 3(1)(8a) of Directive 2013/36/EU and supervisory (non-executive) functions according to Article 3(1)(8) of that Directive[13].

9. 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.

10. In Member States where the management body delegates, partially or fully the executive functions to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons who perform those executive functions on the basis of that delegation should be understood as constituting the management function of the management body in accordance with Article 3(1)(8a) of Directive 2013/36/EU. For the purposes of these guidelines, any reference 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 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.

11. 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.

12. In accordance with Directive 2013/36/EU, Title I, Title II Section 2, Title III Section 7.2, Title IV Section 8, 9, and Section 13, Title V and Title VII (with the exception of paragraphs 244 and 245) apply to third-country branches[14].

13. 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.

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

[14] Additional sections may apply as determined by competent authorities or national law.

## Definitions

14. 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 and all members of the management body of an institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to Directive 2013/36/EU. |
| **Chief executive officer (CEO)** | means the person who is responsible for managing and steering the overall business activities of an institution. |
| **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.[15] |
| **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 |

[15] 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

| | |
|---|---|
| | (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[16]. |
| **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 an institution to deliver critical or important functions through disruption. |

# 3. Implementation

## Date of application

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

## Repeal

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

[16] 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).

# 4. Guidelines

## Title I – Proportionality

17. 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.

18. 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.

19. For the purpose of the application of the principle of proportionality, and 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 use of third-party services providers;

l. the use of different distribution channels;

m. the existing information and communication technology (ICT) systems, including continuity systems;

n. 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; and

o. whether third-country branches as defined under Article 48b of Directive 2013/36/EU are 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

20. 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.

21. Without prejudice of the overall responsibility of the management body, the duties and responsibilities 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 should be described in a written document and duly approved by the management body as specified under paragraphs 71 and 75. 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. 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.

22. 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.

23. 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 risk management, compliance and internal audit functions that have sufficient authority, stature and resources to perform their role;

        ii. includes effective processes to identify, assess, manage, monitor, mitigate 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;

        iii. includes effective operational resilience approach including network and information systems that are established and managed in accordance with Regulation (EU) 2022/2554, and ensuring that organisational arrangements support the continuity of critical or important functions in the event of disruptions;

        iv. 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 Directive 2013/36/EU, 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[17];

h. a selection and suitability assessment process for key function holders[18];

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 8 of these guidelines, which addresses the institution's risk awareness and risk-taking behaviour;

k. a corporate culture and values in line with Section 9, which foster responsible and ethical behaviour, including a code of conduct or similar instrument, diversity and inclusion;

l. a conflict-of-interest policy at institutional level in line with Section 10 and for staff in line with Section 11;

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;

24. When setting, approving and overseeing the implementation of the aspects listed in paragraph 23, 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 financial and non-financial risks in the short, medium and long-term.

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

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

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

26. 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.

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 23 and 24. The internal governance framework and its implementation should be reviewed and updated on a periodic basis, taking into account the proportionality principle, as further specified 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.

30. A member of the management body in its management function may be responsible for an internal control function[19] including in situations where the compliance and risk management functions are combined, provided that the member does not have other roles or responsibilities that would compromise the member's internal control activities and the independence of the internal control functions.

31. 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 regularly inform 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.

32. 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

[19] As referred to in Title IV, Section 10, Title V sections 18.1 and 18.3 of the present guidelines.

with this directive, including the corresponding AML/CFT policies and procedures in the institution and at the level of the management body[20].

# 3 Supervisory function of the management body

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

34. 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 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.

35. 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,

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

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

36. 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.

37. 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.

38. 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 cannot exercise simultaneously the function of a CEO within the same institution. As a general principle, the chair of the management body should be a non-executive member. Where the chair is permitted to assume executive functions including in another entity within the group, the institution should have measures in place to identify, assess and mitigate, where relevant, any adverse impact on the institution's checks and balances, including by appropriately managing conflicts of interests, for example by designating a senior or lead independent board member, or through other appropriate governance arrangements, such as ensuring a sufficiently strong presence of non-executive members within the management body.[21]

39. The chair should set meeting agendas and ensure that strategic issues are discussed as a matter of 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 a timely manner before the meeting.

40. 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

[21] This is a non exhaustive list of examples provided by BCBS principles on corporate governance published in 2015 and and institutions can implement other appropriate safeguard measures.

41. 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 significant, considering the individual, sub-consolidated and consolidated levels, must establish risk, nomination[22] and remuneration[23] 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 institution that is significant in a sub-consolidated or consolidated situation, are not obliged to establish those committees.

42. 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.

43. 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).

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

45. 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.

46. Committees should support the supervisory function of the management body 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[24]

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

48. Independent members[25] of the management body in its supervisory function should be actively involved in committees.

49. 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.

[22] 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.

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

[24] 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.

[25] 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.

50. 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.

51. 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.

52. 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[26]. The remuneration committee should be composed in accordance with the EBA guidelines on sound remuneration policies[27].

53. Members of the remuneration committee should have, individually and collectively appropriate knowledge, skills and experience to assess the impact of risks on remuneration incentives taking into account the assessment of the risk committee as specified under paragraph 64.

54. In G-SIIs and O-SIIs, the nomination committee should include a sufficient number 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, where possible; such institutions may also consider as a good practice having a chair of the nomination committee who is independent.

55. 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.

56. 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, where possible, 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.

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

[26] 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.

[27] EBA guidelines on sound remuneration policies under Directive 2013/36/EU.

## 5.3 Committees' processes

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

59. Committees should interact with each other as appropriate. Without prejudice to paragraph 50, 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.

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

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

62. 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[28], 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

63. 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,

[28] 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),particularly in relation to cross-border groups and in the context of identifying serious breaches of anti-money laundering rules.

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, and 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[29]. 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.

64. 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 factors, related targets or key performance indicators that should be taken into account in the remuneration policy and for performance measurement.

65. 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.

[29] 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

66. In accordance with Directive 2006/43/EC[30], 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[31], 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

    i. receive and take into account audit reports.

[30] 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.

[31] 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).

### 5.6 Combined committees

67. 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.

68. 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.

69. 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[32].

# Title III – Governance framework

# 6 Organisational framework and structure

## 6.1 Organisational framework

70. 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 management body should also ensure that the institution maintains 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.

#### Mapping of duties

71. Institutions should draw up, maintain and update, in accordance with Article 88(3) of Directive 2013/36/EU, in a single set of documents or a repository, a mapping of the individual duties of the persons within the institution who are part of the governance arrangements as referred to in Article 74(1) of Directive 2013/36/EU. The mapping of duties should be appropriate for the size and nature, organisational structure and complexity of the institution and enable it

[32] 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.

to identify any gaps between the roles and the activities covered by the institution, ensuring a clear understanding of how the management and internal governance arrangements of the institution are structured and operate.

72. The management body should approve the mapping of duties. The mapping should be submitted to the competent authorities in due time upon request. The mapping of duties should be available for each institution at individual level and, where applicable, at consolidated and sub-consolidated level. Within groups, institutions may hold the needed information in central systems as long as subsidiaries can access the information relevant to them.

73. The mapping of duties should be coherent with the individual statements of roles and duties as referred to in paragraph 75. It should:

    a. provide a clear overview how roles and duties allocated in an individual statement fit into the overall management body responsibilities and governance arrangements as referred to in Article 74 (1) CRD, and

    b. include sufficient information to allow the identification of any gaps between the individual roles and the activities of the institution.

74. The mapping of duties[33] should include:

    a. a summary of roles, indicating also whether the role is split between two or more persons, and duties of all members of the management body, senior management and key function holders;

    b. information on how the management body both in its management function and in its supervisory function and its committees contribute to the decision making of the management body or bodies;

    c. 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 reporting lines within institutions of the group;

### Individual statements

75. Without prejudice to the overall responsibility of the management body, the individual statements should set out the individual roles and duties and what they entail for each member of the management body in its management function, senior management and each key function holder.

[33] An Annex with a non mandatory template has been provided. Intitutions may decide to use it adapting it to their own specificities.

a. Institutions should ensure that each member of the management body in its management function, senior management and key function holders has a documented statement of their individual role and the allocated duties. The statement should be concise but sufficiently detailed to ensure clarity of the individual's responsibilities.

b. The allocation of role(s) and duties in the individual statements does not exempt any member of the management body in its management function from their collective roles and duties as members of the management body. Where 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 same institution, only one statement of roles and duties is required. Where roles held in more than one institution, including within a group, an individual statement should be drawn up for each institution.

c. The individual statement of roles and duties should be kept up-to-date taking into account the review of the mapping of duties and be signed by the individual it applies to and submitted to competence authorities upon request in accordance with Article 88(3) of Directive 2013/36/EU.

76. The institution should take appropriate measures to ensure that all individuals appropriately fulfil their duties.

## 6.2 Know your structure

77. 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.

78. 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.

79. 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.

80. 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.

81. 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

82. 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[34]. 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[35];

[34] 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.

[35] 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

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.

83. 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.

84. When setting up such structures, the management body should understand them and their purpose and the 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.

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

86. 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:

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.

87. 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.

88. 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

## 7.1 Application in a group context

89. 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[36]. 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.

90. 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.

91. 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

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

separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. 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

98. Third-country branches should implement a robust and sound governance framework in accordance with Articles 48g and 74 of Directive 2013/36/EU, taking into account the criteria for the application of the proportionality set out in Title I [37].

99. 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 32, where applicable, taking into account the specific nature of third-country branches. 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 32, where applicable, taking into account the specific nature of third country branches. The local management committee should comply with the open discussion and documentation requirements referred to in paragraphs 60 and 61.

100. 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 undertakings in the third country or another group entity. 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.

101. In line with Article 76(6) of Directive 2013/36/EU as applied to third-country branches pursuant to Article 48g thereof, 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.

102. Where third country-branches are required to apply the requirements of Article 76(6) third subparagraph 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

[37] References to the "management body" in these Guidelines should be intended as to the two persons or more located in the relevant Member State effectively directing the business of third-country branches or local management committee, where established, according to Article 48g of Directive 2013/36/EU.

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.

103. Third-country branches should maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities', including when using third-party services providers supporting critical or important functions, or executing back-to-back transactions or any other service arrangement 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;

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 supporting critical or important functions; and

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

104. The use of third-party arrangements including intragroup arrangements and third-party service providers located in third countries to support critical or important functions 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[38].

105. Third-country branches should manage their ICT risks in accordance with Article 48g of Directive 2013/36/EU and Regulation (EU) 2022/2554 (DORA)[39].

106. When relying on back-to-back booking arrangements, third country branches should ensure at a minimum, that transactions with an EU nexus 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.

107. Without prejudice to Article 48g(2) and (3) of Directive 2013/36/EU, third-country branches should comply with the remuneration principles set out in Articles 92, 94 and 95 of Directive

[38] Please refer to the Regulation (EU) 2022/2554 in particular regarding ICT third party risk management and the EBA guidelines on third party risk management

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

2013/36/EU [40] and the EBA guidelines on sound remuneration policies under Directive 2013/36/EU. Third country branches should be able to provide all the necessary information and documents where necessary to ensure that remuneration principles are being complied with.

# Title IV – Risk culture and business conduct

## 8 Risk culture

108. 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.

109. 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.

110. 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.

111. 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.

112. 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 institution's 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 formalised 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

[40] 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.

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[41].

# 9 Corporate values and code of conduct

113. The management body should develop, adopt, adhere to and promote high ethical and professional standards, considering 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.

114. Institutions should establish a culture of equality, diversity and inclusion and prevent discrimination and harassment. 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.

115. 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 opportunities[42] for all staff independent of their genders, including with regard to career perspectives and aim to improve the representation of the underrepresented gender in

[41] Please refer also to the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU (EBA/GL/2021/04), available at https://www.eba.europa.eu/regulation-and-policy/remuneration.

[42] 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.

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).[43] Where the recruitment process includes selection committees, those should have as a general principle a gender balanced composition. 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.

116. Institutions should use additional internal 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. The implemented standards should aim at enhancing the institution's robust governance arrangements and reducing the risks to which the institution is exposed 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.

117. 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 8 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

[43] See also EBA Guidelines on sound remuneration policies under Directive 2013/36/EU.

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.

118. 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.

## 10 Conflict of interest policy at institutional level

119. 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.

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

121. 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.

122. 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. Where CEO simultaneously holds a position as a member of the management body in its supervisory function (including Chair) in different institutions within the same group, institutions should have measures in place to assess any potential conflicts of interests and, where identified, apply and document appropriate mitigation measures.

123. Without prejudice to national law, institutions should ensure that where a former CEO becomes chairperson within the same entity within two years after their executive mandate has ended, any potential conflicts of interest are appropriately identified, managed and mitigated as appropriate.

124. Where such a transition takes place without a cooling-off period of two years, institutions should put in place appropriate measures to address potential conflicts of interest, in particular where the individual would oversee, as a chairperson, decisions or actions taken during their former executive role. Such measures may include, but are not limited to one or more of 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 conflict of interest.

    b. If deemed necessary, the chair 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 where a conflict of interest has been identified.

    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 cannot participate in the discussion, nor take part in the vote.

## 11 Conflict of interest policy for staff[44]

125. 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.

126. 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.

127. 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.

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

[44] 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.

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;

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.

129. 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.

130. 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.

131. 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.

132. 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.

133. 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[45].

134. 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.

135. 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.

136. 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.

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

137. As part of their conflicts of interest policies for staff (Section 11) and the management of conflicts of interest as set out in paragraph 134, the management body should set out a framework for identifying and managing conflicts of interest in the context of granting loans

[45]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.

and entering into other transactions (e.g. factoring, leasing, property transactions, etc.) with members of the management body and their related parties.

138. Without prejudice to the national transposition of Directive 2013/36/EU46, 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.

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

140. 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 [47] 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.

141. 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.

142. 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.

143. 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.

144. 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

[46] Please also refer to Basel Core Principle 20.

[47] 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).

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.

145. 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.

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

146. For the purpose of Article 88(1) of Directive 2013/36/EU, institutions should document data on loans[48] 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.

147. 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.

148. 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:

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

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[49]; and

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.

## 12 Internal alert procedures

149. 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.

150. 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) 2016/67950 (GDPR).

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

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

[50] 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).

Institutions may also provide for a whistleblowing process that allows information to be submitted in an anonymised way.

152. 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.

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

154. 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.

## 13 Reporting of breaches to competent authorities

155. 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 12;

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 12.

156. 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

## 14 Internal control framework

157. 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.

158. 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.

159. 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.

160. 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, services provided by third-party services providers and distribution channels.

161. 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.

## 15 Implementing an internal control framework

162. 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.

163. 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.

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

165. 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.

166. 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.

167. 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.

## 16 Risk management framework

168. 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 relevant categories of financial and non-financial risks. In accordance with Article 87a of the Directive 2013/36/EU, the risk management framework should pay also 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.

169. 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.

170. 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.

171. 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.

172. 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.

173. 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.

174. 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.

175. 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).

176. 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.

177. 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.

178. 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.

## 17 New products and significant changes[51]

179. 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 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.

180. 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).

181. 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.

182. 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

[51] 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.

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.

183. 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 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. 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.

## 18 Internal control functions

184. In accordance with Article 76(5) of Directive 2013/36/EU, the internal control functions should include a risk management function (see Section 19), a compliance function (see Section 20) and an internal audit function (see Section 21). 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 ensuring compliance with AML/CTF requirements.

185. The operational tasks of the internal control functions may be performed by a third-party service provider, taking into account the proportionality criteria listed in Title I, which maybe 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 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.

186. As part of the internal control functions, in accordance with Article 11(1) of Regulation (EU) 2024/1624 [52], institutions should assign the responsibility for ensuring the institution's

[52] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Applies from 10 July 2027.

compliance with the requirements of that Regulation and the institution's policies and procedures to a member of the management body in its management function[53]. The person responsible for the policies, procedures and controls in the day-to-day operation of the obliged entity's AML/CFT requirements in accordance with Article 11(2) and 11(5) of Regulation (EU) 2024/1624, should, be able to directly report to the management body in its supervisory function and raise concern where specific risk developments affect or may affect the institution.

## 18.1 Heads of the internal control functions

187. 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 their responsibilities. Where in accordance with Article 76(6) of Directive 2013/36/EU, and under conditions referred under paragraph 30, an internal control function is headed by a member of the management body in its management function, the institution should ensure that appropriate safeguards and mitigants are in place to avoid conflicts of interest, such as but not limited to, an independent mindset of the individual and appropriate key performance indicators, including objective appraisal and remuneration determination.

188. The heads of internal control functions should have direct access and can report directly to the management body in its supervisory function. They should be able to raise concerns and warn the supervisory function, where appropriate, or where specific risk developments affect or can 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 71 and 75.

189. Institutions should have documented processes as referred to in paragraph 71 in place to assign the position of the head of an internal control function and for withdrawing 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.

## 18.2 Independence of internal control functions

190. In accordance with Article 76 paragraphs 5 and 6 of Directive 2013/36/EU, institutions should have internal control functions independent from the operational functions and from the members of the management body in its management function and from senior management. This independence should not prevent internal control functions from interacting with business lines. Internal control functions should have direct access and can

[53] Please refer also to the EBA Guidelines on the role, tasks and responsibilities AML/CFT compliance officer .

report directly 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.

191. For the internal control functions to be regarded as independent as per paragraph 190, 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 should not otherwise compromise their objectivity[54].

## 18.3 Combination of internal control functions

192. Taking into account the proportionality criteria set out in Title I, the risk management function and the compliance function may be combined. In this regard, in accordance with Article 76(6), third subparagraph of Directive 2013/36/EU and paragraphs 30 and 187 of these guidelines, institutions should be able to demonstrate that, considering the nature, scale and complexity of their activities, the appointment of separate person for each function is not justified. Institutions should ensure that the required conflict of interest assessment has been performed and that any identified conflicts of interest are appropriately mitigated. The decision to combine the risk management function with the compliance function should be duly documented. It should be ensured that the senior person fulfils the suitability criteria including time commitment and requirements of knowledge, skills and experience laid out in Article 76(6) of Directive (EU) 2013/36/EU. The internal audit function cannot be combined with another internal control function.

## 18.4 Resources of internal control functions

[54] 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.

193. 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.

194. 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.

# 19 Risk management function

195. Institutions should establish a risk management function (RMF) covering the whole institution. The RMF should have sufficient authority and stature taking into account the proportionality criteria listed in Title I, to implement risk policies and the risk management framework as set out in Section 16.

196. 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. 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.

197. 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.

198. 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.

199. 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.

200. 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.

## 19.1 RMF's role in risk strategy and decisions

201. 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.

202. 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.

## 19.2 RMF's role in material changes

203. In line with Section 17, 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.

204. 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.

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

205. 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.

206. 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.

207. 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.

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

209. 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 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.

210. 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.

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

## 19.4 RMF's role in unapproved exposures

212. 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.

213. 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.

## 19.5 Head of the risk management function

214. 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.

215. The head of the RMF should have sufficient expertise, independence and seniority to challenge decisions that affect an institution's exposure to risks.

216. 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.

217. 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.

## 20 Compliance function

218. Institutions should establish a permanent and effective compliance function to identify manage and mitigate compliance risk and ensure that the institution's risk strategy and all material management decisions take into account risk stemming from non-compliance events. The head of compliance function should be responsible for this function across the entire institution (the compliance officer or head of compliance).

219. 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.

220. 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.

221. 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.

222. 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 risk stemming from non-compliance 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.

223. In line with Section 17 of these guidelines, the compliance function should also verify, in close cooperation with the RMF and the legal unit, that new products, new systems and new procedures comply with the current legal framework and, where appropriate, with any known forthcoming changes to legislation, regulations and supervisory requirements.

224. 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).

225. 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.

## 21 Internal audit function

226. 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.

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

228. 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 services provided by third-party service providers, with the institution's policies and procedures and with regulatory requirements. Each entity within the group should fall within the scope of the IAF.

229. 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.

230. 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 14 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 business units acting as the first line of defence and the risk management and compliance functions.

231. 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.

232. 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.

233. 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.

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

235. 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.

236. 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

237. Institutions should establish a sound business continuity management, encompassing appropriate planning and 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[55], in particular the ICT business continuity policy adopted according to Article 11 (1) of Regulation (EU) 2022/2554 and should contribute to the institution's

[55] 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.

operational resilience by ensuring coordinated preparedness across functions, resources and third-party arrangements.

238. 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.

239. In order to establish a sound business continuity management, an institution should perform a business impact analysis to identify and measure (quantitatively and qualitatively) the potential impact of severe business disruptions, using internal and external data and scenario analysis. This analysis should cover all business lines and internal units, including the RMF, and should take into account key interdependencies. The results of the analysis should contribute to defining the institution's recovery priorities and objectives.

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

a. business continuity and contingency plans to ensure the institution would be able to react appropriately to disruptions and to maintain its critical or important functions in case of disruption; and

b. response and recovery plans for critical 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.

241. Business continuity, contingency, response and recovery plans should be documented and carefully implemented and subject to internal audit review. The documentation should be available to the staff involved in the execution of the plans and should be stored on systems that are physically separated and readily accessible in case of emergency. Appropriate operational resilience and business continuity awareness, including training, should be provided. Plans should be regularly tested and updated. Testing results should be documented, analysed, reported to the management body and be used to review the plans accordingly.

## Title VII – Transparency

242. 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.

243. 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.

244. 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[56], by country.

245. 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.

[56] 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 – 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'[57]) 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 annex

[57]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):*<br>*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 entry into force of Directive 2019/878/EU. The update of the Guidelines is needed following the entry into force of Directive (EU) 2024/1619. Consistency with other EBA regulatory product should also be ensured.
3. The 2026 amendments to the guidelines aim at:

- specifying further the requirements introduced by Article 48g of Directive (EU) 2013/36 on third country branches' sound internal governance arrangements, taking into account third country branches specificities and the application of proportionality.
- ensuring 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.
- ensuring that the simplification and burden reduction objectives are implemented as stated in the EBA action plan (TFE Recommendation 2.2) endorsed by the EBA Board of Supervisors in December 2025 while preserving sound governance arrangements.

### B. Baseline scenario

4. 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 the EBA Guidelines on management of ESG risks.

5. The impact assessment covers the guidelines developed to ensure a consistent and harmonised application of additional governance requirements applicable to institutions 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

### Changes made in 2026 [58]

6. Directive (EU) 2024/1619 (CRD VI) introduces amendments to Directive 2013/36/EU to ensure that third-country branches have sound internal governance arrangements. These requirements form part of the harmonised framework for third-country branches established within the EU, which was introduced in light of the material footprint that some of these branches have in the EU banking sector and the resulting risks to financial stability in the EU, as well as the currently fragmented prudential and supervisory requirements to which they were subject. The impact of the introduction of those requirements into the Directive has been assessed in the legislative process and is not considered in this impact assessment.

7. While the specifications regarding the requirements for third country branches in the Guidelines are new, third-country branches were already expected to comply with internal governance requirements and were already in the scope of the Guidelines on internal governance published in 2021. Certain aspects 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 of Directive 2013/36/EU. In this context, the implementation and compliance costs resulting from the additional clarifications provided by the Guidelines are expected to be limited.

8. CRD VI also introduced a requirement that institutions need 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, senior management and key function holders. The Guidelines provide additional details on how these individual statements should be prepared, taking into account a proportionate approach, and include an optional template in the Annex. The options of not providing a template and of introducing a mandatory template were both considered but ultimately disregarded to provide institutions with as much guidance as possible while limiting the potential constraints associated with a mandatory template. Given that the preparation of individual statements is already a requirement under the Directive, and that the template is optional, the costs resulting from these additional clarifications provided by the Guidelines are expected to be limited. In addition, all the required information to complete the necessary documentation is already available within institutions.

[58] For the previous amendments to the Guidelines made in 2021 and earlier, please refer to the impact assessments of those versions of the Guidelines that are available on the EBA's website.

9. Similarly, institutions are required to draw up, maintain and update a mapping of duties, including details of reporting lines, areas of responsibility and the persons involved in the governance arrangements. Given that the mapping of duties depends on institutions' organisational structures and specific characteristics, no template was considered appropriate for this requirement. The approach is principles-based and provides institutions with the flexibility to present the mapping of duties in the manner they consider most appropriate, provided that the relevant guidance is complied with. Given that the mapping of duties is already a requirement under the Directive 2013/36/EU, the costs resulting from these additional clarifications provided by the Guidelines are expected to be negligible. Furthermore, all the relevant information is already available within institutions.

10. The Guidelines also required the redrafting of certain sections to reflect the findings of the EBA benchmarking report on diversity practices and gender-neutral remuneration policies, the consideration of ESG risks in the short, medium and long term within the prudential framework in accordance with Article 87a of Directive 2013/36/EU and the EBA Guidelines on the management of ESG risks, as well as the changes resulting from the entry into force of the digital operational resilience framework under Regulation (EU) 2022/2554. These changes are not expected to entail significant implementation costs, as they primarily ensure consistency with new or existing regulatory requirements.

### Simplification and burden reduction

11. The revised Guidelines are expected to contribute to simplification and burden reduction objectives while preserving the underlying prudential objectives. In response to stakeholders' feedback, several provisions have been streamlined, reformulated at a higher level and made more principles based. The revised text places greater emphasis on proportionality, allowing institutions and third-country branches to implement the requirements in a manner that is commensurate with their size, internal organisation, and the nature, scope and complexity of their activities.

12. Administrative burden is reduced through, among other measures, the possibility of relying on existing repositories of governance documents, including within the group, for the preparation and maintenance of individual statements and mappings of duties, the removal of duplicative or overly prescriptive requirements, the deletion of provisions that overlap with existing regulatory frameworks, and the simplification of diversity and inclusion monitoring expectations. The clarification of the scope of application for third-country branches and the more targeted approach to conflicts of interest are expected to enhance legal certainty and facilitate implementation.

## D. Cost-benefit analysis

13. Given the limited amendments introduced by CRD VI regarding governance arrangements, the changes to the Guidelines are expected to result in no, or only very limited, implementation costs for third-country branches and for institutions with regard to the implantation of

individual statements and mapping of duties. Furthermore, regarding individual statements and mapping of duties the information required is already available within institutions, which further limits any additional compliance and operational costs.

14. In line with the simplification and burden reduction objectives and taking into account the application of the principle of proportionality, the Guidelines provide institutions with sufficient flexibility in the implementation of the governance requirements and avoid imposing unnecessary administrative burdens, including through the use of an optional template for individual statements and a principles-based approach for the mapping of duties.

15. While a limited implementation effort may be required to review governance frameworks and adapt internal documentation where necessary, the resulting costs are expected to be low. This is because most of the requirements either reflect obligations already introduced by Directive 2013/36/EU or clarify existing supervisory expectations. In addition, the relevant information and governance arrangements are already available within institutions and third-country branches in most cases. The revised Guidelines have been updated considering implementation burden reduction. Compared with the consultation draft, the final text adopts a more principles-based and proportionate approach, removes unnecessary prescriptiveness and simplifies a number of requirements.

16. Additional burden-reduction measures include the deletion of Annex I, which largely duplicated provisions already contained in the main body of the Guidelines, the removal of the standalone section on the general policy for third-party risk management, which is already covered by dedicated regulatory frameworks, and the simplification of diversity and inclusion provisions through a less prescriptive and more principles-based approach. These changes are expected to reduce compliance costs and administrative burdens, particularly for smaller and non-complex institutions.

17. The revised Guidelines also improve proportionality and legal certainty. For third-country branches, the clearer distinction between applicable and non-applicable provisions and the more targeted application of governance requirements are expected to facilitate implementation and supervisory assessment. Similarly, the clarification of conflict-of-interest provisions and the more targeted cooling-off framework provide greater flexibility while maintaining appropriate safeguards. These clarifications reduce uncertainty and may lower implementation and interpretation costs for institutions and supervisors.

18. The Guidelines improve clarity, consistency and supervisory convergence across the Union, while preserving the key prudential objectives of sound governance, clear accountability and effective risk management.

19. Overall, the revised Guidelines provide a more operational and proportionate framework, reducing compliance costs and implementation efforts for institutions and competent authorities without compromising supervisory effectiveness or governance standards.

## 5.2. Views of the Banking Stakeholder Group (BSG)59

The Banking Stakeholder Group (BSG) stresses that the guidelines should be interpreted with broad flexibility, taking into account not only the size, complexity, and risk profile of institutions, but also the diversity of national governance frameworks and board structures across the European Union. They consider that the principle of proportionality is fundamental and should allow institutions to design their governance structures in a manner proportionate to their specific circumstances. According to the BSG, certain sections of the guidelines are overly prescriptive and detailed and could hinder the ability of management to respond efficiently to changing business needs.

The group suggests that the mapping of duties and individual statements requirements are burdensome without improving governance quality. BSG recommends a more principle-based approach, asserting that existing documentation such as organisational charts and job descriptions should be sufficient to meet regulatory expectations.

Regarding board roles and executive functions, the BSG advises that flexibility should be retained for the chair of the management body to assume executive functions, provided that appropriate checks and balances are in place. They warn against imposing a uniform governance model that does not reflect the diversity of legal frameworks across Member States. Furthermore, the BSG argues that stricter requirements on the compatibility of roles within groups and the introduction of a three-year cooling-off period go beyond the requirements of CRD VI and may conflict with national law.

The BSG also finds the requirement for both individual and collective ESG expertise for remuneration committee members unnecessarily strict and inconsistent with other EBA guidelines, suggesting that collective knowledge should be sufficient.

They support the monitoring of gender diversity but recommend that the list of KPIs be reviewed to avoid overlap with other regulations, such as the CSRD and Pay Transparency Directive, and that institutions should have the flexibility to select indicators appropriate to their context.

The group requests clarification that the compliance function should be responsible for "compliance risk" rather than the broader "legal risk," to avoid confusion with the responsibilities of the legal department.

The BSG also questions the requirement for BCP documentation to be stored on "physically separated systems," as this is not found in DORA or other EBA guidelines and may cause ambiguity.

[59] The full BSG response is available under: https://www.eba.europa.eu/publications-and-media/events/consultation-revised-guidelines-internal-governance-under-crd

## 5.3. Feedback on the public consultation and on the opinion of the Banking Stakeholder Group (BSG)

The EBA publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for 3 month and ended on 7 November 2025. 24 responses were received, of which 22 were published on the EBA website, the other 2 were submitted confidentially. The BSG also submitted its opinion.

This paper presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases several industry bodies made similar comments, or the same body repeated its comments in the response to different questions. In such cases, the comments, and EBA analysis are included in the section of this paper where EBA considers them most appropriate.

Changes to the draft Guidelines been incorporated as a result of the responses received during the public consultation.

### Summary of key issues and the EBA's response

Stakeholders broadly supported the principle of proportionality but requested clearer criteria, such as size or complexity, to determine simplified governance requirements. Concerns were raised about disproportionate compliance costs for small institutions.

Several respondents objected to removing references to national company law and called for reinstating definitions for key roles like CEO and heads of control functions.

On management bodies and committees, stakeholders welcomed clarification of roles but found mapping duties and individual statements too granular. Annex II's mapping requirements were criticized as overly detailed. Respondents suggested using existing documentation and limiting mapping to management functions.

Restrictions on intra-group roles and cooling-off periods for former CEOs were strongly opposed as exceeding CRD VI and reducing flexibility. Most called for deletion or revision of these provisions.

On ESG and risk management, stakeholders agreed on integration but warned against disproportionate emphasis. Respondents opposed mandatory individual ESG expertise in remuneration committees, preferring collective competence and flexibility in composition. Stakeholders supported gender-neutral policies but requested flexibility in monitoring and reporting.

For third-country branches, stakeholders supported harmonization, but highlighted challenges in applying all requirements considering that branches are not having their own legal personality. They

sought clarity on 'sufficient presence,' delegation, and proportionality, noting that not all group-level rules should apply.

Internal control functions' independence was supported, but requirements were seen as rigid. Respondents requested flexibility in combining risk and compliance roles and objected to terminology changes that blurred distinctions between compliance and legal functions.

Business continuity requirements were generally supported, but respondents sought clarification on terms and consistency with DORA.

### EBA' response

The EBA Guidelines aim to specify further the provisions under the governance provisions of Directive 2023/36/EU (CRD) as amended by Directive (EU) 2024/1619 (CRD VI).

The Guidelines apply in a proportionate way and remain open to different national company law.

Definitions removed from the Guidelines are largely directly included in the Directives and apply also in the context of these Guidelines.

While institutions are required to more gender neutrality and diversity, the indicators included represent examples and good practices rather than a mandatory list of indicators to be implemented. However, to introduce a more proportionate approach, the indicators have been removed.

Regarding the business continuity requirements, the Guidelines have been closer aligned with DORA and the BCBS principles, given the different context, i.e. general high-level principles versus more detailed specific ICT related requirements that apply under DORA, some more general language has been used.

The provisions on the mapping of duties, interplay between compliance and legal function, and conflicts of interest have been reviewed and comments taken into account where appropriate while ensuring that sound governance arrangements are preserved.

The EBA's responses to the more detailed comments are included in the below feedback-table.

## Summary of responses to the consultation and the EBA's analysis

| Comments | Summary of responses received | EBA analysis | Amendments to the proposals |
|---|---|---|---|
| **General comments** | | | |
| Level of detail and consistency with national law | Some respondents recommended to provide principle-based guidance rather than prescriptive rules, especially where national practices vary, in particular national company law | The EBA GL specify further the requirements set within Directive 2013/36/EU (CRD) with an aim of harmonisation. MS are required to implement the CRD into national law. Guidelines specify the CRD provisions. A certain level of detail within the GL is required to achieve harmonisation, however, institutions remain responsible for their internal organisation and therefore the GL should not be overly prescriptive. In particular, the EBA GL is not prescriptive regarding the governance system chosen by institutions or prescribed under national company law and allows for different systems, e.g. 1-tier or 2-tier systems. | No change |
| Overlap with other EU Regulations | Respondents pointed out that the EBA GL overlap with other EU Regulations like DORA, CSRD, Pay Transparency Directive. | Given the different scope of application and the mandate within CRD to provide the CRD's governance provisions, a certain overlap of requirements cannot be avoided. However, the EBA aimed at consistency between the different frameworks. | No change |

| | | | |
|---|---|---|---|
| Consistent regulatory framework | A few respondents recommended to coordinate better between EBA and ECB Guidelines "Guide on Risk Culture Governance". | The Guidelines are based on the CRD. ECB guides have a different nature than EBA Guidelines and apply only within the Banking Union. ECB-SSM is also subject to the comply or explain process and ECB guides should be in line with EBA regulatory products. ECB-SSM as a CA participates to the development of our guidelines. | No change |
| Scope of KFH | Respondents view that CRD VI applies suitability assessments not to all Key Function Holders, but the heads of the internal control functions and CFO, only remain subject to both internal (by the bank) and external (by the supervisor) fit and proper assessments.<br><br>Respondents state that Art. 91a (5) explicitly limits the scope of external supervisory screening to the heads of internal control function and the CFO. Based on the institution's definition of KFH, a broader group of people may fall within this category, which suggests that banks are expected to conduct internal assessments for a broader group than those subject to external supervisory screening. | The suitability requirements in Art. 91a(1) CRD apply to all Key Function Holders (KFH) and entities need in line with par. 2 of this Article ensure that KFH fulfill at all times the suitability requirements. "Key function holders" means the persons who have significant influence over the direction of an institution but are not members of the management body, including the heads of internal control functions and the chief financial officer, where those heads or that officer are not members of the management body.<br><br>Competent authorities are required to assess certain KFH but are able to assess also the suitability of other KFHs.<br><br>Guidelines cannot change the approach to KFH assessments introduced in CRD. | No change |

| | | | |
|---|---|---|---|
| ESG | Some respondents consider that the GL gives to much focus on ESG data and risk management. | The requirement to consider ESG risk factors has been introduced by CRD VI, the GL reflect the respective provisions. | GL amended |
| **Responses to questions in Consultation Paper EBA/CP/20xx/xx** | | | |
| Question 1 | | | |
| 5a | A few respondents suggest adding a reference to central bodies. "….as well as to central bodies as referred to in Article 10 of Regulation (EU) No 575/2013." | The comment has been accommodated. | GL amended |
| Par 6 | A few respondents find that the application of the Guidelines on internal governance to network and information systems in accordance with Regulation (EU) 2022/2554 (DORA) leads to a lack of clarity, given that DORA is already highly detailed. | The Guidelines specify the internal governance arrangement of institutions, the amended Article 74 (1)(d) CRD explicitly refers to network and information systems, which fall therefore in the scope of application of the governance provisions under CRD in parallel to the DORA requirements. | No change |
| Footnote 14, Par 6 | The rationale is not clear considering that par. 6 refers to all risks. | Institutions must manage all their risks. However, the purpose of the footnote is to highlight those risk categories that have recently received more regulatory focus. | No change |
| Par.7 | A few respondent have suggested that paragraph 7 be amended as follows: "[…] | The comment has been accommodated. | GL amended |

| | | | |
|---|---|---|---|
| | 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) functions when acting as a "management body in its management function" and as having supervisory (non-executive) functions when acting as a "management body in its supervisory functions" as those terms are defined, respectively, in points (8a) and (8) of that article." | | |
| Par 8 | Some respondents comment that in 1-tier systems, it is not feasible to individualise responsibilities as suggested in the draft Guidelines, for example by allocating duties to non-executive members or distinguishing between management and supervisory functions. | The Guidelines follows the definitions provided within CRD. While in unitary boards, members all have an overall responsibility, there are management functions and supervisory functions present in the management body. A differentiation usually can be made based on the duties allocated to members of the management body. | No change |
| Par 8 | Respondents find the paragraph too prescriptive. Flexibility should be interpreted broadly, covering not only the size, complexity and risk profile of institutions, but also the diversity of national governance frameworks across | The paragraph does clarify that the term management body, as defined in CRD, applies to the GL but need to be interpreted in the context of national laws. The last sentence has been reinstated. | GL amended |

| | | | |
|---|---|---|---|
| | the EU. Specifically, it is suggested to retain the last sentence of par 8. | | |
| Par 9. and<br><br>section 2 | Many respondents comment that this paragraph should maintain the reference to the possibility of delegating the management function to an internal executive body, as it provides clarity and certainty in Member States where the law allows such delegation of management functions of the management body. | Guidelines have been maintained. In many institutions executive committees exist where not all members have the power to effectively direct the business of the institution but instead have powers only in certain areas. Such members are not necessarily members of the management body. They may include senior management and KFHs, who are also subject to suitability assessments, but through different processes and, to some extent, different criteria compared with those applied to members of the management body. The GL has been clarified | GL amended<br><br>GLs amended |
| Par 11 | A few respondents suggest clarifying or re-insert definitions for heads of internal control functions and key function holders and restore the statement that CEO/CFO/KFH definitions are functional and do not in itself require the creation of such positions. | Definitions are now included in the Directives have been removed from the Guidelines. It goes without saying that a definition in itself does not form a requirement to establish the defined functions. | No change |
| Definitions<br><br>Paragraph 13 | Some respondents remark that the definition of “operational resilience” is consistent with the definition proposed in the draft Guidelines on the sound management of third-party risk (non-ICT | DORA is targeted to the digital operational resilience while the definition in these guidelines is not limited to digital operational resilience and covers a broader scope in line with BCBS standards. | No change |

| | | | |
|---|---|---|---|
| | related services), but that it does not coincide with that of "digital operational resilience" introduced by the DORA Regulation. Therefore, it would be preferable the definition adopted in the Guidelines be aligned with that contained in DORA Regulation.<br><br>A few respondents ask for the exact definition of the term group. | Article 4(1) point 138 of Regulation (EU) 575/2013 defines the term group. ‘ | |
| Definition | | | |
| Date of application | Respondents comment that the CRD VI is to be transposed by Member States only by 10 January 2026 and that therefore the CP might cause interpretation and implementation challenges for institutions and could risk national fragmentation in the implementation of the Guidelines. A clear date should be set, and institutions should be given sufficient time to implement the Guidelines | The legislator provided deadlines for some parts of the mandates covered by the Guidelines. An early consultation provides for sufficient transparency regarding specifications provided by the GL. The GL will only enter into force after the transposition deadline; a date of application is included in each set of guidelines published by the EBA. CRD does not include grandfathering or transitional periods regarding this matter. | No change |
| Question 2 | | | |
| Title I – Proportionality<br><br>Paragraph 16 | Many respondents request a clearer and broader application of the proportionality principle, emphasizing that governance | The principle of proportionality applies with regard to the application of all provisions and all entities within the scope of application and is not limited to specific | No change |

| | | | |
|---|---|---|---|
| | requirements should be tailored to the size, complexity, and business model of institutions.<br><br>A few respondents find that the level of detail of the GL and their prescriptiveness limits the application of proportionality. | company forms. However, the application of proportionality does not create any derogations/exemptions from CRD provisions.<br><br>A certain level of detail of Guidelines to specify further the CRD provisions and to ensure a level playing field is necessary. The GL have been reviewed based on the submission of comments and taking into account simplification objectives. | |
| Title II – Role and composition of the management body and committees | Multiple comments argue that the guidelines are prescriptive regarding separation of functions, conflicts of interest, and committee composition, warning this may restrict organisational flexibility and commenting that the Guidelines go beyond CRD VI, especially before national transposition. | Please refer to the specific comments. Some amendments have been made to the Guidelines to reduce their complexity and introduce a more proportionate approach. | GL amended |
| Paragraph 20 | Some respondents ask for clarification that mapping of duties and individual statements apply only to the management body in its management function, not the supervisory function. | Article 88 (3) CRD requires that "…Member States shall ensure that institutions 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 as referred to in Article 74(1) and of their duties" Based on European Commission clarification, mapping of duties applies to all members of the management body- executive and supervisory functions. | GL clarified |

| | | | |
|---|---|---|---|
| Paragraph 22 c | Some respondents question the removal of the term "independent" for internal control functions and the explicit mention of concentration risk from exposures to central counterparties, suggesting these changes are unclear or unnecessary. | The wording “independent” has been reinstated and does need to be repeated all the time.<br><br>Article 81 CRD refers explicitly to those concentration risks, the GL have been updated for consistency reasons. | GL amended |
| Paragraph 22 c.<br><br>subpoint i(b) | Some respondents comment that this paragraph is not in line with DORA, which in Article 5 states that the purpose of having in place an internal governance and control framework “ensures effective and prudent management of ICT risk (…) in order to achieve a high level of digital operational resilience.” Different drafting suggestions have been received. | Network and information system fall under the amended Article 74 CRD and the management body‘s responsibilities, including ensuring their compliance with DORA. The wording has been clarified. | GL amended |
| 23 | Single respondents suggest for the sake of clarity to define the terms “traditional categories of financial and non-financial risks” and “potential materialisation of operational and legal risks”. | The paragraph has been clarified. | GL amended |
| Paragraph 29a | Some respondents suggest clarifying the language regarding members of the management body being responsible for internal control functions, especially | The combination of mandates of members of the management body and head of internal control function is possible in accordance with Article 76 (6) of the CRD and subject to the principle of proportionality. | GL amended. |

| | | | |
|---|---|---|---|
| | regarding segregation of duties and conflict of interest. | A reference to the section on conflicts of interest management has been added. | |
| Par 29 a | A few respondents comment that "mandate" is not the adequate terminology if we want to address the case of a member of the management body in charge of private banking, credit, trading room or any other risk-taking function that would be incompatible with an ICF role.<br><br>Respondents note that paragraph 29a should refer only to Section 19.1 (paragraph 172) of the Guidelines, which governs the appointment of heads of internal control functions and allows such functions to be headed by a member of the management body in its management function. Respondents further note that Section 19.3 (paragraph 176) concerns the combination of internal control functions and, following CRD VI, the combination with other tasks performed by a "senior person" under Article 76(6) CRD, a concept which—pursuant to Article 3(1)(9) CRD—excludes members of the management body. Respondents | The term "mandate" has been replaced by "roles or responsibilities".<br><br>The term "senior person" is not defined within CRD. CRD defines as correctly stated the term "senior management". Sentence 1 of the 3rd subpar of Article 76(6) specifies that "the heads of internal control functions shall be independent senior managers". Under certain conditions this subparagraph allows the appointment of another "senior person" (the word another making clear that this need not be a senior manager). Where this is the case, that senior person may fulfil the responsibilities for the compliance or risk management functions and therefore the reference to par 19.3 has been added as the combination of those functions remains possible under this scenario. | GLs amended |

| | | | |
|---|---|---|---|
| | therefore suggest limiting the reference in paragraph 29a to Section 19.1 only. | | |
| Paragraph 33 | Some respondents question the legal basis for requiring independent members on the supervisory body. | In the view of the EBA the existence of independent directors, in particular for large institutions, are an element of sound governance arrangements under Article 74 CRD. The provision is also consistent with the corresponding BCBS Guidelines. | No change |
| Paragraph 37 | Many respondents argue that the guidelines should not prohibit the chair of the management body from holding executive functions, provided appropriate checks and balances are in place. | The Guidelines have been clarified. | GL amended |
| Paragraph 51 | Numerous respondents consider the requirement for individual ESG expertise for remuneration committee members excessive, advocating for collective knowledge instead. | The requirement of individual knowledge, skills and experience has been removed and the reference to risk appetite regarding ESG risks has been deleted. | GL amended. |
| | A few others suggest that this requirement should be removed as the incentives should take into account the resulting risks of ESG factors in terms of capital and liquidity in particular. | Key performance indicators for staff in this context are not limited to changes of capital and liquidity as a consequence of ESG factors, which may include other indicators, e.g. customer satisfaction, volume targets on green loans etc. | |

| | | | |
|---|---|---|---|
| Paragraph 61 (c) | Several respondents question the inclusion of "fundamental rights" and "discrimination" as operational risks overseen by the risk committee, suggesting these are compliance matters or should be clarified. Some respondents suggest deleting the examples “(including legal and IT, fundamental rights, discrimination and ICT risks)”. | The examples have been deleted as they only represent a small part of what falls under operational risks. | GL amended |
| Paragraph 62 | Many respondents argue there is no legal basis for requiring the risk committee to provide input to the remuneration committee regarding ESG risks and related KPIs. | The second subparagraph of Article 76(4) CRD as amended by CRD VI specifically requires “…the establishment of sound remuneration policies and practices, the risk committee shall, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration system take into consideration risks, including those resulting from the impacts of ESG factors, capital, liquidity and the likelihood and timing of earnings.’<br><br>Considering the above, as part of robust governance arrangements risk and remuneration committees, where established, must cooperate also regarding relevant ESG factors, including related KPI and reflect such factors in the remuneration system. | No change |
| Question 3 | | | |

| | | | |
|---|---|---|---|
| Paragraph 68 | One respondent asked to clarify if the referred "substance" is intended as economic substance as in the rest of the Guidelines | The term substance is not linked to the economic substance, but to the presence of a sufficient physical presence and resources in the EU that ensure that the institution can be effectively supervised and meets the requirements under CRD. | No change |
| Title III – Governance framework<br><br>Section 6 | Many respondents are concerned and comment that requirements for mapping of duties and individual statements are overly detailed, burdensome, and go beyond CRD VI as it is not compatible with the overall responsibility of members of the management body.<br><br>Many are recommending allowing reliance on existing documentation (for example, organisation charts, regulation on the Internal Control System, etc.). In particular a specific format (Annex II) is not necessary and adds extra burden.<br><br>A few respondents ask to leave the responsibility for the approval of such documents to the entity or allow it to be delegated to the management function or senior management for their direct reporting lines. | The guidance has been revised and simplified. Under Article 88(3) CRD, the mapping of duties concerns all persons that are part of the institutions governance arrangements. The mapping complements the institution's existing governance framework which explains its governance arrangements, how its governing bodies are structured and interact, and its organisational chart. This is without prejudice of the overall responsibility of the management body as a collegial body in accordance with CRD.<br><br>The Guidelines require an approval of the management body as they have the responsibility for the institution's overall governance arrangements.<br><br>The mapping of duties has to be updated, if needed (e.g. to align with changes in individual statements). Such updates do not require a full new approval process where changes are limited or minor. | GL amended |

| | | | |
|---|---|---|---|
| | A few respondents find the regular update of those statements too burdensome, e.g. where new persons take over an existing position. | | |
| Level of application of mapping of duties | Some respondents request that the guidelines clarify the scope of application at consolidated/group level. | CRD applies to institutions defined in point (3) of Article 4(1) of Regulation (EU) 575/2013. Article 3(3) CRD specifies that CRD applies also on a consolidated or sub-consolidated basis. Article 88(3) CRD applies as specified above on an individual and on a consolidated or (where applicable) sub-consolidated basis. | No change |
| Mapping of duties | Single respondent suggests that the mapping of duties requirement could not be applicable where Article 91(14) CRD VI applies, i.e. where regional or local elected bodies are involved, or where the management body lacks selection authority. | The CRD in Article 91(14) CRD provisions do not provide for a derogation from Article 88(3) CRD in case of members appointed by regional or local elected bodies. The requirements have therefore to be applied. | No change |
| Paragraphs 68 a, b and c: | One respondent required to clarify whether:<br><br>(1) the mapping of duty and individual statement of duties is to be rendered public outside of the organisation or is to be seen as an internal document and | The mapping of duties serves internal and supervisory purposes. The 2nd subparagraph of Article 88(3) specifies that "Member States shall ensure that the individual statements of duties and the mapping of duties are made available at all times and communicated, including to obtain authorisation as set out in Article 8, in due time, upon request, to the competent authorities." | No change |

| | | | |
|---|---|---|---|
| Par 68.a.c. | A respondent suggests deleting the 2nd part of the par as it is too detailed: "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." | Paragraph has been amended and clarified. | GL amended |
| 68 a.f. | One respondent asks for acknowledging the institutions' right to draw up and maintain the mapping of duties in a set of documents or a repository to avoid duplicities between internal documents and reduce the administrative burden. | The mapping is to ensure that institutions have a complete overview of all duties and how these are allocated throughout their organisation. This is not always clearly covered by the existing documents. Institutions do not have to make a separate, single document but can have a repository of documents that provides a clear overview. | No change |
| Par 68 a.f. (ii) | One respondent points out that the management body itself is the corporate body authorised to adopt decisions pursuant to national law. There is no rationale for this requirement. | The comment has been accommodated. | GL amended |

| | | | |
|---|---|---|---|
| Paragraph 68(a)(f)(iii): | One respondent asked to clarify whether the mapping of duties should identify roles rather than named individuals, given that traceability to specific persons is already ensured through internal nomination processes and signed individual statements of duties, and that naming individuals would add complexity and quickly become outdated. | The comment has been accommodated even if institutions should be able to provide to competent authorities the names of all members of the management body, senior management and KFH. | GL amended |
| Paragraph 68a.f.(v).and (vi) | One respondent considers that smaller institutions typically have fewer employees, with individuals often performing multiple functions, reflecting a necessary proportionality in their organisational setup, the combination of roles should be reflected in the mapping of duties. | The Guidelines have been amended to reflect the comments made. | GL amended |
| Paragraph 68.a.g. | A few respondents comment that this provision should be deleted because it goes beyond what is required according to Art. 88(3) CRD VI, which only requires institutions to prepare documentation and keep it updated. | The management body is responsible for the internal organisation of the institution and bears the responsibility for the mapping of duties. The guidelines have been amended. | GL clarified |
| Paragraph 68.b.a. | A few respondents commented that the indication of the expected time | The comment has been accommodated | GL amended |

| | | | |
|---|---|---|---|
| | commitment should remain part of the FAP assessments | | |
| Paragraph 68.b.b. | Respondents recommended rephrasing the first sentence to reflect the overarching principle of collective responsibility of the management body.<br><br>Furthermore, please delete the second sentence. This sentence is unnecessary, as the suitability requirements already cover the expectation that members of the management body in its management function possess appropriate knowledge and contribute effectively. | The comments have been clarified and the suggestion accommodated. | GL amended |
| 68.b.b | One respondent suggests providing an exemption for group situations where an individual holds roles in multiple group entities, given that requiring a separate individual statement for each institution appears disproportionate. | The requirement applies on an individual and consolidated- or sub-consolidated level. Guidelines cannot provide derogations from CRD provisions. | No change |
| Paragraph 68.b.d. | Some respondents find the requirement is disproportionate as any person could only assume the respective role after the passing of the suitability assessment and recommend deleting it. | It should be noted that some Member States apply ex-post assessments that may benefit from the individual statements and mapping of duties. | GL amended |

| | | | |
|---|---|---|---|
| | It conflicts with data privacy law (e.g. principle of data minimization (Art. 5 GDPR)) as sensitive personal data are concerned.<br><br>The signature requirement goes beyond what is required according to Art. 88 (3) of Directive 2013/36/EU.<br><br>One respondent also asked for clarification as to what is meant by "in due time" per Article 88(3) CRD VI to ensure consistent supervisory expectations across Member States. | The GDPR allows processing of data where there is a legal basis, which is given by the need to assess the suitability of e.g. members of the management body<br><br>The documentation to be submitted to competent authorities for large entities will be set out in the RTS on documentation.<br><br>It is difficult to reconcile why an individual statement should not be validated by a signature of the person making such statement.<br><br>A timely submission of documents to competent authorities is a precondition for being effectively supervised. Competent authorities will specify the expected timelines in line with supervisory practices. | |
| Paragraph 68.c | Respondents pointed out that Article 88(3) of Directive (EU) 2024/1619 only requires the establishment of individual statements of responsibilities and a mapping of duties and does not introduce a burden of proof on individuals. They argued that paragraph 68c appears to introduce such a regime. | The Guidelines have been revised with a view of simplifying the provisions. | GL amended |
| Question 4 | Third Country Branches | | |

| | | | |
|---|---|---|---|
| Section 7 – Organisational framework in a group context | Some respondents request clarification on the definition of "group". | The term group is defined in Regulation (EU)575/2013 (CRR) and applies to the present Guidelines, the CRR also specifies the scope of consolidation.<br><br>Please refer also to the Q&As published on the EBAs website already regarding Article 18 CRR and the Commission Delegated Regulation (EU) 2022/676 of 3 December 2021 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council with regard to regulatory technical standards specifying the conditions in accordance with which consolidation is to be carried out in the cases referred to in Article 18(3) to (6) and Article 18(8) of that Regulation (Text with EEA relevance). | No change |
| Scope of application | It is not clear enough in the guidelines what is applicable to the third-country branches (only this specific section, or other parts). | The Guidelines specify the provisions applicable to third-country branches in the relevant dedicated section (see scope of application of the guidelines). | No change |
| Clarity | A few respondents commented that to ensure consistent implementation, it would be helpful to clarify whether presence refers to physical location, decision-making authority, or operational control. | 'Presence' refers to having a physical location in the Member State, and the persons effectively directing the business being present at the premises of the third-country branch to an extent that they are able to effectively fulfil their role. TBC should have sufficient resources locally but taking into account the application of the proportionality principle. | No change |

| | | | |
|---|---|---|---|
| Section 7.2 | Few respondents argued that the Guidelines do not sufficiently reflect proportionality. While retaining overall responsibility, the respondent suggested allowing delegation of day-to-day supervisory functions, for example to regional general managers or delegated governance fora. The respondent further requested explicit clarification that third-country branches are expected to apply the Guidelines proportionately, in line with Section 7.2 and Article 48g CRD VI. | The Guidelines do not require the management body in its management function of the head undertaking to run the day-to-day business of a third-country branch, neither to have a management body in its management function but describe the requirement of Article 48g of Directive 2013/36/EU for the branch to have at least two persons located in the relevant Member State effectively directing the business of the third-country branch. These persons should have similar duties and responsibilities as members of the management body in its management function.<br><br>As the third-country branch has not the legal personality from a legal perspective, it is not required to have a management body in its supervisory function. The Guidelines explain already that the proportionality principle as set out in Title I applies. | Gl amended |
| Par 90 (g) | A few respondents find the term “service agreements and transactions” problematic as the branch cannot enter into a contract and suggest finding a more neutral wording. | The wording has been revised and the paragraph updated. | Gl amended |
| Paragraph 90j | Respondents noted that Article 48g(2) CRD requires third-country branches to | The Guidelines have been amended to reflect the comments made. | GL amended |

| | | | |
|---|---|---|---|
| | comply with Articles 92, 94 and 95 CRD only, which do not include Article 93 nor a reference to the EBA Guidelines on sound remuneration policies. They therefore suggested amending paragraph 90j to refer solely to compliance with Articles 92, 94 and 95 CRD and the EBA Guidelines on sound remuneration policies, as specified. | | |
| Paragraph 90h | One respondent claims that paragraph 90h should not assume full DORA applicability to third-country branches. | Q&A 102 has been published and clarifies the applicability of DORA. Accordingly, DORA applies to third-country branches in line with the relevant provisions of the CRD and DORA, and paragraph 90h does not assume applicability beyond the legal framework in force. | No change |
| Paragraph 90i | One respondent suggests that first part of the para: "third country branches should ensure at a minimum, transactions with an EU nexus are neither systematically nor substantially back-to-backed, and are risk-managed from the EU", goes beyond the requirements in CRD VI and may have a negative impact on branches' pricing models | The guidelines have been clarified. | GI amended |

| | | | |
|---|---|---|---|
| Section 8 – Third-party risk management policy | Several respondents suggest cross-referencing the EBA Guidelines on third-party risk management for clarity. | The Section on TPRM has been deleted and cross reference to TPRM GLs made. | |
| Question 5 | | | |
| Title IV – Risk culture and business conduct | Many respondents express concern that the guidelines go beyond CRD VI by introducing new restrictions on intra-group roles, conflicts of interest, and cooling-off periods. | The GL reflect changes made to CRD. There are no additional restrictions included in the GL that go beyond the ones introduced by CRD. The GL set out the additional measures to be taken where such situations exist that indeed cause conflicts of interest. | No change |
| Paragraph 101a | A respondent raises concern about the prescriptive list of gender diversity indicators, with recommendations to keep indicator selection at the institution's discretion and avoid overlap with other regulations (e.g., CSRD, Pay Transparency Directive | The list of indicators has been deleted. | GLs amended |
| Paragraph 102 | The proposed drafting result in a slight broadening of scope and introduces the concept of "professional standards". We would welcome further guidance from the EBA on the underlying objective: does this amendment aim to expand the range of aspects to be covered (e.g. beyond sustainability, responsibility and | The wording has been clarified | GL amended |

| | | | |
|---|---|---|---|
| | resilience), and how should "professional standards" be interpreted in this context? | | |
| Paragraphs 107a–107b | Many comments oppose the introduction of restrictions on the compatibility of roles (e.g., CEO of a subsidiary as Chair of the parent) and the three-year cooling-off period, arguing these go beyond CRD VI. This concerns, e.g. the access of CEOs to the Board of directors within Groups. Some of them suggest deleting par 107a completely as it goes beyond the CRD requirements. | With the aim to have a simpler and proportionate approach, the guidelines have been amended narrowing the scope to CEO and Chair to specify further Article 88 par. 1 of CRD; the cooling-off period has also been reduced. | GL amended |
| | Some respondents point to the privileged counting of directorships within groups and argue that this demonstrates that this should not be considered a conflict of interest. | Counting of directorships relates to time commitment rather than conflicts of interest. | No change |
| | Paragraph 107a one respondent states that the impact on “the duty to oversee their own previous actions” is not clear since the paragraph refers to functions exercised simultaneously. | The guidelines have been clarified. | GL amended |
| Par 107 c | A few respondents suggest the deletion of this paragraph as it is already covered by the general rules on the duty of loyalty. | This is an example to mitigate conflicts of interests. Even when already considered to be part of duty of loyalty, it is a way to manage the conflict of interest. | No change |

Question 6

| | | | |
|---|---|---|---|
| Paragraph 152 | Some respondents caution that the guidelines' emphasis on ESG risks should not detract from the importance of traditional risk categories (credit, market, liquidity). They recommend that ESG risks be addressed equally, not as a special focus. | In line with the CRD amendments introduced by CRD VI, ESG risks are risk factors and do not form a risk category for which capital or liquidity reserves must be held. The guidelines have been clarified. | GL amended |
| Paragraph 171 | Some respondents requested clarification on how the concepts of "compliance manager" and "compliance officer" under Regulation (EU) 2024/1624 (AMLR) are reflected in paragraph 171. While the first sentence is understood to refer to the "compliance manager" as defined in Article 11(1) AMLR, it is unclear whether the "separate AML/CFT compliance function" referred to in the second sentence corresponds to the "compliance officer" under Article 11(2) AMLR or to a different role. | The wording has been clarified.<br><br>The wording has been clarified. | GL amended<br><br>GL amended |
| Paragraph 172 | Several respondents note that combining the role of head of control functions with that of the management body or with other functions presents different | The combination of mandates of members of the management body and head of internal control function is possible in accordance with Article 76 (6) of the CRD and subject to the principle of proportionality. | No change |

| | | | |
|---|---|---|---|
| | conflict-of-interest risks and should be addressed accordingly. | This reading has been confirmed by the European Commission. A reference to the section on conflicts of interest management has been added. The guidelines have been streamlined. | |
| Paragraph 176 | Some respondents ask for on the combination of internal control functions and the conditions under which this is permissible, especially for small institutions. Respondents therefore suggested aligning paragraph 176 more closely with Article 76(6) CRD by clearly distinguishing between the combination of internal control functions and the entrustment of either function to another senior person, and by clarifying the applicable conditions, documentation and safeguards, including conflict-of-interest assessments and suitability requirements. | Risk management function and compliance function may be combined taking into account the application of proportionality. These functions may be combined by another senior person within the organisation including by a member of the management body in its management function. The guidelines have been clarified. | GL clarified |
| Paragraph 187 | Some respondents suggest reformulating: "The RMF should provide the management body with all relevant information to establish ESG risk-related strategies, policies and plans in line with the EBA guidelines on the management of environmental, social and governance | The guidelines have been amended. This section deals with all the risks that institutions are or might be exposed to. | GL amended |

| | | | |
|---|---|---|---|
| | (ESG) risks (EBA GL/2025/01), particularly section 6." | | |
| Paragraph 195 - | It is not clear why ICT related information is added to this specific paragraph. Furthermore "ICT-related information" is not defined. Please remove the proposed part of the sentence | The comment has been accommodated. | GL amended |
| Par 205 and 206 | Some respondents propose to retain the proportionality approach introduced by those paragraphs and allow for the combination of functions as currently applied. | This is now under para 176 | No change |
| Paragraph 215 | Respondents considered that the removal of the last sentence in 215 is not comprehensible in line with the clarification on paragraph 176 (that 'The internal audit function must not be combined with any other business line or another (internal control) function.'). | The paragraph has been reinstated | GLs amended |
| Question 7 | | | |
| Title VI – Business continuity management | Respondents request clarification that references to "recovery" and "recovery plans" refer to disaster recovery/business | The comment has been accommodated and the guidelines clarified. | GL amended |

| | | | |
|---|---|---|---|
| | continuity, not financial recovery under the BRRD. | | |
| Paragraph 230 | Respondents considered that the addition of the wording “and subject to internal audit review” in the first sentence of paragraph 230 is unnecessary and should be deleted. They also noted that the reference to documentation being stored on “physically separated systems” may create interpretative uncertainty, as this concept is not explicitly reflected in DORA or in the EBA Guidelines on ICT risk management and security. Respondents therefore suggested reformulating or removing this reference to ensure alignment with DORA. | Business continuity, contingency, response and recovery plans should be documented and subject to internal audit review.<br><br>The documentation should be stored on systems that are physically separated and readily accessible in case of emergency. This is in line with an effective operational resilience framework. | No change<br><br>No change |
| Annex II – Optional template for individual statements of roles and duties | Many respondents argue that the annex is too detailed and risks being interpreted as binding. They recommend that any template should be optional and that institutions should be allowed to use existing documentation formats. | The Annex should be kept as individual statements are new a requirement introduced by CRD 6. This annex is not mandatory but helps to ensure supervisory convergence. Annex I instead has been deleted. | GL amended |