EBA/CP/2020/20

31/07/2020

Consultation Paper

Draft Guidelines

on internal governance under Directive 2013/36/EU

Contents

Responding to this consultation

The EBA invites comments solely on the amendments to the EBA Guidelines on Internal Governance put forward in this paper, as shown in track changes and within the questions summarised in 5.2.

The amendments are minor and aim at bringing the Guidelines in line with Directive 2013/36/EUDirective 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[1] as in force after the amendments witha Directive (EU) 2019/878 of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures[2] and Directive (EU) 2019/2034 of the European Parliament of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU[3].

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 31 October 2020. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

[1] OJ L 176, 27.6.2013, p. 338

[2] OJ L 150, 07/06/2019, p. 253

[3] OJ L 314, 05/12/2019, [. 64

Data protection

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

Executive Summary

In recent years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct credit institutions' weak or superficial internal governance practices, as identified during the financial crisis. Recently, there has been a greater focus on conduct-related shortcomings and activities in offshore financial centres.

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

To further harmonise credit institutions' internal governance arrangements, processes and mechanisms within the EU in line with the requirements introduced by Directive 2013/36/EU, the European Banking Authority (EBA) is mandated by Article 74(3) of Directive 2013/36/EU, to develop guidelines in this area. The guidelines apply to all credit institutions regardless of their governance structures (unitary board, dual board or other structure), without advocating or preferring any specific structure, as set out specifically in the scope of application. The guidelines apply in the same way as to credit institutions to 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. The terms 'management body in its management function' and 'management body in its supervisory function' should be interpreted throughout the guidelines in accordance with the applicable law within each Member State.

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

The guidelines are based on an earlier set of guidelines on internal governance and in particular add additional requirements that aim to foster a sound risk culture implemented by the management body, to strengthen the management body's oversight of the credit institution's activities and to strengthen the risk management frameworks of credit institutions. Additional guidelines have been provided to further increase the transparency of credit institutions' offshore activities and to ensure the consideration of risks within credit institutions' change processes.

Next steps

The EBA will finalise its updated guidelines on internal governance after the public consultation. It is expected that the amended Guidelines will enter into force on 26 June 2021 .

Background and rationale

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

2. In recent years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct credit institutions' weak or superficial internal governance practices, as identified during the financial crisis. These faulty practices, while not a direct trigger for the financial crisis, were closely associated with it and were questionable. In addition, recently, there has been a greater focus on conduct-related shortcomings and activities in offshore financial centres.

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

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

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

6. Against this background, there is a clear need to address the potentially detrimental effects of poorly designed internal governance arrangements on the sound management of risk, to ensure effective oversight by the management body, in particular in its supervisory function, to promote a sound risk culture at all levels of credit institutions and to enable competent authorities to supervise and monitor the adequacy of internal governance arrangements.

Legal basis

7. All legal references in this document should be understood as reflecting the situation as of 26 June 2021, i.e. reference is made to Directive 2013/36/EU [4] as amended by Directive 2019/878/EU [5] and by Directive 2019/2034/EU [6]; the same holds true for references to Regulation (EU) No 575/2013 [7] that should be understood as Regulation (EU) No 575/2013 as amended by Regulation (EU) 2019/876 [8] of the European Parliament and of the Council of 20 May 2019 and by Regulation 2019/2033/EU [9].

8. The guidelines apply in the same way as to credit institutions to 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.

9. To further harmonise credit institutions' internal governance arrangements, processes and mechanisms within the EU, the EBA is mandated by Article 74(3) of Directive 2013/36/EU to develop guidelines in this area.

10. Article 74(1) of Directive 2013/36/EU, requires credit institutions to have robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility.

11. Article 76 of Directive 2013/36/EU sets out requirements for the involvement of the management body in risk management, the setting up of a risk committee for significant credit institutions, and the tasks and organisation of the risk management function. In addition, this Article establishes 'that the head of the risk management function shall be an independent senior management with distinct responsibility for the risk management function'. To reflect the wording of the Directive, the revised guidelines refer, regarding the second line of defence, to the '(independent) risk management function', while the previous guidelines used the term '(independent) risk control function'. However, it should be

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

[5] Directive (EU) 2019/878 of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures

[6] Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU.

[7] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit credit institutions and investment firms and amending Regulation (EU) No 648/2012

[8] Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013 as regards the leverage ratio, the net stable funding ratio, requirements for own funds and eligible liabilities, counterparty credit risk, market risk, exposures to central counterparties, exposures to collective investment undertakings, large exposures, reporting and disclosure requirements, and Regulation (EU) No 648/2012

[9] Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014

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 credit institution.

12. Article 88 of Directive 2013/36/EU sets out the responsibilities of the management body regarding governance arrangements and the obligation to set up a nomination committee for significant credit institutions.

13. Under Article 109(1) of Directive 2013/36/EU, competent authorities must require credit 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 as amended by Regulation (EU) 2019/876 and/or waivers for credit institutions permanently affiliated to a central body in compliance with Article 21 of Directive 2013/36/EU.

14. Under Article 109 (2) of Directive 2013/36/EU these guidelines apply on a sub-consolidated and 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 adequate. 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 offshore financial centres. These arrangements, processes and mechanisms must also be consistent and well-integrated and those subsidiaries not subject to this Directive must also be able to produce any data and information relevant to the purpose of supervision

15. According to 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 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[10].

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

17. In line with Article 47 of Directive 2013/36/EU, branches in a Member State of credit credit institutions authorised in a third country should be subject to equivalent requirements to those applicable to credit institutions within the Member State where the branch is located,

[10] See EBA guidelines on sound remuneration policies

taking into account regarding internal governance arrangements that the branch does not have a management body but persons who are responsible for effectively directing the business.

18. The guidelines should be read in conjunction with and without prejudice to the EBA guidelines on sound remuneration policies and the joint EBA and ESMA guidelines on the assessment of the suitability of members of the management body and key function holders].

19. These guidelines should be read in conjunction with other relevant EBA publications, including the EBA guidelines on outsourcing arrangements , the EBA guidelines on the supervisory review process and the EBA guidelines on disclosures.

Rationale and objective of the guidelines

20. Internal governance includes all standards and principles concerned with setting an credit institution's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined and clearly allocated; 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 technology systems, outsourcing arrangements and business continuity management.

21. Combating money laundering and terrorist financing is essential for maintaining stability and integrity in the financial system. Uncovering involvement of a credit 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 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 clarifies 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.

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

23. In addition, it is also necessary to take into account developments in this area since the publication of the revised EBA guidelines on internal governance in 2017, such as the updated OECD principles of corporate governance[11] and the revised corporate governance principles

[11] The OECD principles can be found at http://www.oecd.org/corporate/principles-corporate-governance.htm.

for banks published by the Basel Committee on Banking Supervision (BCBS)[12]. The guidelines align the terminology used regarding risk appetite and risk tolerance with the EBA guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and also with the revised BCBS principles; they use the term 'risk appetite' to refer to the aggregate level of risk and the types of risk an credit institution is willing to assume, while 'risk capacity' is the maximum amount of risk an credit institution is able to assume.

24. 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.

25. 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.

26. 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 on the basis of that delegation should be understood as constituting 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 executive body or the CEO, as defined in these guidelines, even if they have not been proposed or appointed as formal members of the credit institution's governing body or bodies under national law.

27. The management body is empowered to set the credit institution's strategy, objectives and overall direction, and oversees and monitors management decision-making. The management body in its management function directs the credit institution. Senior management is accountable to the management body for the day-to-day running of the credit institution. The management body in its supervisory function oversees and challenges the management function and provides appropriate advice. The oversight roles include reviewing the performance of the management function and the achievement of objectives, challenging the strategy, and monitoring and scrutinising the systems that ensure the integrity of financial information as well as the soundness and effectiveness of risk management and internal controls.

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

28. 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.

29. Independent directors within the supervisory function of the management body helps to ensure that the interests of all internal and external stakeholders are considered and that independent judgement is exercised where there is an actual or potential conflict of interest[13].

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

31. The guidelines use the so-called 'three lines of defence' model in identifying the functions within credit institutions responsible for addressing and managing risks.

32. The business lines, as 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 credit institution's risk appetite and that the business activities are in compliance with external and internal requirements.

33. The risk management function and compliance function form the second line of defence. The risk management function (referred to in the previous guidelines as the 'risk control function') facilitates the implementation of a sound risk management framework throughout the credit institution and has responsibility for further identifying, monitoring, analysing, measuring, managing and reporting on risks and forming a holistic view on all risks on an individual and consolidated basis. It challenges and assists in the implementation of risk management measures by the business lines in order to ensure that the process and controls in place at the first line of defence are properly designed and effective. The compliance function monitors compliance with legal 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 risks and to ensure compliance. Both functions may intervene to ensure the modification of internal control and risk management systems within the first line of defence where necessary.

[13] 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. The independent 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 in charge also of the independent review of the first two lines of defence. The internal audit function performs its tasks fully independently of the other lines of defence.

35. 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, and report directly to the management body. 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.

36. All requirements 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 credit institution's size, internal organisation and nature, and the complexity of its activities.

37. The guidelines specify requirements under Directive 2013/36/EU that need to be considered when setting up new structures, e.g. in 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 credit institutions on governance arrangements, including in relation to such structures.

38. The guidelines aim to establish a sound risk culture in credit institutions. Risks should be taken within a well-defined framework in line with the credit institution's risk strategy and 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 credit institutions' products, processes and systems, are to be duly identified, assessed, appropriately managed and monitored. The risk management function and compliance function should be involved in the establishment of the framework and the approval of such changes to ensure that all material risks are taken into account and that the credit institution complies with all internal and external requirements.

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

40. Loans to members of the management body and their related parties are a specific source of actual or potential conflicts of interests and specific requirements have been explicitly included in Article 88 (1) of Directive 2013/36/EU regarding such loans. In the same way also other transactions with members of the management body and their related parties have the

potential to create conflicts of interests and therefore guidelines for theappropriate management of such conflicts of interests are provided.

EBA/CP/2020

DD Month YYYY

Draft Guidelines

on internal governance

1. Compliance and reporting obligations

Status of these guidelines

1. These guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010[14]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authority and financial institutions, including credit 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 credit 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/xxx'. 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.

[14] 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 the internal governance arrangements, processes and mechanisms that credit institutions that are subject to Directive 2013/36/EU[15], as amended by Directive 2019/878/EU[16], must implement in accordance with Article 74(1) of Directive 2013/36/EU to ensure effective and prudent management of the credit institution.

Addressees

6. These guidelines are addressed to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013[17], as amended by Regulation (EU) 2019/876 [18], including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013, and to credit institutions as defined in point 1 of Article 4(1) of Regulation (EU) No 575/2013.

Scope of application

7. These guidelines apply in relation to credit institutions' governance arrangements, including their organisational structure and the corresponding lines of responsibility, processes to identify, manage, monitor and report all risks[19] they are or might be exposed to, and internal control framework. The guidelines should also apply in the same way to 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[20]. Each reference to credit institutions should be understood as including such investment firms.

[15] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit credit institutions and the prudential supervision of credit 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).

[16] Directive (EU) 2019/878 of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures.

[17] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1-337).

[18] Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013 as regards the leverage ratio, the net stable funding ratio, requirements for own funds and eligible liabilities, counterparty credit risk, market risk, exposures to central counterparties, exposures to collective investment undertakings, large exposures, reporting and disclosure requirements, and Regulation (EU) No 648/2012.

[19] Any reference to risks in these guidelines should include money laundering and terrorist financing risks.

[20] Regulation (EU) 2019/2033 of the European Parliament and f the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014

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 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 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[21].

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

13. Credit institutions should comply and competent authorities should ensure that credit 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.

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

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 credit 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 credit institution is able to assume given its capital base, its risk management and control capabilities, and its regulatory constraints.
Risk culture	means an credit institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume.
Staff	means all employees of an credit institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to Directive 2013/36/EU, and all members of the management body in its management function and in its supervisory function.
Chief executive officer (CEO)	means the person who is responsible for managing and steering the overall business activities of an credit institution.
Chief financial officer (CFO)	means the person who is overall responsible for managing all of the following activities: financial resources management, financial planning and financial reporting.
Heads of internal control functions	means the persons at the highest hierarchical level in charge of effectively managing the day-to-day operation of the independent risk management, compliance and internal audit functions.
Key function holders	means persons who have significant influence over the direction of the credit institution but who are not members of the management body and are not the CEO. They include the heads of internal control functions and the CFO, where they are not members of the management body, and, where identified on a risk-based approach by credit institutions, other key function holders. Other key function holders might include heads of significant business lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions.

Prudential consolidation	means the application of the prudential rules set out in Directive 2013/36/EU and Regulation (EU) No 575/2013 on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013.
Consolidating credit institution	means a credit 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 credit institutions	means credit institutions referred to in Article 131 of Directive 2013/36/EU (global systemically important credit institutions (G-SIIs) and other systemically important credit institutions (O-SIIs)), and, as appropriate, other credit institutions determined by the competent authority or national law, based on an assessment of the credit institutions' size and internal organisation, and the nature, scope and complexity of their activities.
Listed CRD-credit institution	means credit institutions whose financial instruments are admitted to trading on a regulated market or on a multilateral trading facility as defined under Article 4, paragraphs (21) and (22) of Directive 2014/65/EU, in one or more Member States[22].
Shareholder	means a person who owns shares in an credit institution or, depending on the legal form of an credit institution, other owners or members of the credit institution.
Directorship	means a position as a member of the management body of an credit institution or another legal entity.

3. Implementation

Date of application

15. These updated guidelines apply from 26 June 2021 [TBC].

Repeal

16. The EBA Guidelines on internal governance (EBA/GL/2017/11) of 26 September 2017 are repealed with effect from 26 June 2021 [TBC].

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

[22] 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 credit institution, so that the objectives of the regulatory requirements are effectively achieved.

18. Credit 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 credit institutions should have more sophisticated governance arrangements, while small and less complex credit institutions may implement simpler governance arrangements.

19. For the purpose of the application of the principle of proportionality and in order to ensure an appropriate implementation of the requirements, the following criteria should be taken into account by credit institutions and competent authorities:

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

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

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

    d. whether it is a listed credit institution t;

    e. whether the credit 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 credit 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 credit institution's organisational structure;

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

i. the ownership and funding structure of the credit institution;

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

k. the outsourced functions and distribution channels;

l. the existing information technology (IT) systems, including continuity systems and outsourcing functions in this area; and

m. wether the credit institution falls under the definition of a large institution or a small and non-complex credit institution.

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 credit institution and defines, oversees and is accountable for the implementation of the governance arrangements within the credit institution that ensure effective and prudent management of the credit institution.

21. The duties of the management body should be clearly defined, distinguishing between the duties of the management (executive) function and of the supervisory (non-executive) function. The responsibilities and duties of the management body should be described in a written document and duly approved by the management body. All members of the management body should be fully aware of the structure and responsibilities of the management body, and of the division of tasks between different functions of the management body and its committees.

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, its decision-making 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 credit institution within the applicable legal and regulatory framework, taking into account the credit institution's long-term financial interests and solvency;

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

c. an adequate and effective internal governance and internal control framework that includes a clear organisational structure and well-functioning independent internal risk management, compliance and audit functions that have sufficient authority, stature and resources to perform their functions;

d. an adequate and effective internal governance and internal control framework as defined in Title V, to ensure compliance with applicable requirements also in the context of the prevention of money laundering and terrorism financing;

Question 2: Point (d) has been added, throughout the Guidelines references to money laundering and terrorism financing and the institutions obligations have been added, are those references sufficiently clear? The Guidelines aims at clarifying that AML/TF measures form a part of institutions governance arrangements. The EBA is developing further separate work on AML compliance.

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

f. targets for the liquidity management of the credit institution;

g. a remuneration policy that is in line with the remuneration principles set out in Articles 92 to 95 of Directive 2013/36/EU and the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU[23];

h. 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[24];

i. a selection and suitability assessment process for key function holders[25];

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

[23] EBA guidelines on sound remuneration policies

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

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

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;

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

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

m. a conflict of interest policy at credit institutional level in line with Section 11 and for staff in line with Section 12; and

n. 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 sustainable business model that takes into account all risks, including environmental, social and governance risks .

Question 3: Paragraph 24 regarding ESG factors has been added, is it sufficiently clear? The addition is thought as providing a link between the responsibilities of the management body and the aspect of ESG factors. Respondents should be aware that the EBA is developing further detailked work in the area of sustainable finance.

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

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

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

28. 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 25 and 26. The internal governance framework and its

implementation should be reviewed and updated on a periodic basis taking into account the proportionality principle, as further explained in Title I. A deeper review should be carried out where material changes affect the credit institution.

2 Management function of the management body

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

30. 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 credit institution's management.

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 inform regularly and where necessary without undue delay the management body in its supervisory function of the relevant elements for the assessment of a situation, the risks and developments affecting or that may affect the credit institution, e.g. material decisions on business activities and risks taken, the evaluation of the credit institution's economic and business environment, liquidity and sound capital base, and assessment of its material risk exposures.

32. In line with Directive 2015/849/EU[26], credit institutions should assign the responsibility for ensuring the credit institution's compliance with the national implementation of that Directive to a member of the management body in its management function or where such a body does not exist to the person effectively directing the business of the credit institution.

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 credit 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:

[26] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

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 credit 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 credit institution's internal governance framework and take appropriate steps to address any identified deficiencies;

e. oversee and monitor that the credit institution's strategic objectives, organisational structure and risk strategy, including 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 credit institution is implemented consistently;

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

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

i. ensure that the heads of internal control functions are able to act independently and, regardless the responsibility to report to other internal bodies, business lines or units, can raise concerns and warn the management body in its supervisory function directly, where necessary, when adverse risk developments affect or may affect the credit 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, should 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. As a general principle, the chair of the management body should be a non-executive member. Where the chair is permitted to assume executive duties, the credit institution should have measures in place to mitigate any adverse impact on the credit institution's checks and balances (e.g. by designating a lead board member or a senior independent board member, or by having a larger number of non-executive members within the management body in its supervisory function). In particular, in accordance with Article 88(1)(e) of Directive 2013/36/EU, the chair of the management body in its supervisory function of an credit institution must not exercise simultaneously the functions of a CEO within the same credit institution, unless justified by the credit institution and authorised by competent authorities.

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

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

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 credit institutions that are themselves significant, considering the individual, sub-consolidated and consolidated levels, must establish risk, nomination[27] and remuneration[28] committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this body. Non-significant credit institutions, including when they are within the scope of prudential consolidation of an credit institution that is significant in a sub-consolidated or consolidated situation, are not obliged to establish those committees.

[27] 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.

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

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. Credit 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. Credit 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 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[29]

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[30] 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.

50. Credit 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. Credit 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 credit institution concerned. The audit

[29] 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.

[30] 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.

committee should be composed in accordance with Article 41 of Directive 2006/43/EC[31]. The remuneration committee should be composed in accordance with Section 2.4.1 of the EBA guidelines on sound remuneration policies[32].

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

54. Members of the nomination committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning the selection process and suitability requirements.

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

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

5.3 Committees' processes

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

58. 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.

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

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

61. The risk and nomination committees should at least:

[31] 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.

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

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, risk, compliance, including AML/CTF compliance , audit, etc.);

b. receive regular reports, ad hoc information, communications and opinions from heads of internal control functions concerning the current risk profile of the credit institution, its risk culture and its risk limits, as well as on any material breaches[33], 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

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

a. advise and support the management body in its supervisory function regarding the monitoring of the credit institution's overall actual and future risk appetite and strategy, 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 credit institution;

b. assist the management body in its supervisory function in overseeing the implementation of the credit 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 credit institution, such as market, credit, operational (including legal and IT risks), and reputational risks, in order to assess their adequacy against the approved risk appetite and strategy;

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 credit 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;

[33] With regard to serious breaches in the area of AML/TF. please refer also to the Guidelines to be issued under Article 117 (6) of Directive 2013/36/EU, specifying the manner of cooperation and information exchange between the authorities referred to in paragraph 5 of this Article, particularly in relation to cross-border groups and in the context of identifying serious breaches of anti-money laundering rules.

f. review a number of possible scenarios, including stressed scenarios, to assess how the credit 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 credit institution[34]. 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.

63. 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 credit institution's internal control functions, in particular the risk management function.

64. 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 credit institution's risk, capital and liquidity and the likelihood and timing of earnings.

5.5 Role of the audit committee

65. In accordance with Directive 2006/43/EC[35], where established, the audit committee should, inter alia:

a. monitor the effectiveness of the credit 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 credit institution, without breaching its independence;

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

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

[34] 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.

[35] 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.

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[36], and in particular the appropriateness of the provision of non-audit services to the audited credit 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 credit 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.

5.6 Combined committees

66. In accordance with Article 76(3) of Directive 2013/36/EU, competent authorities may allow credit 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.

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

68. Credit 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[37].

[36] 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).

[37] 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.

Title III – Governance framework

6 Organisational framework and structure

6.1 Organisational framework

69. The management body of an credit institution should ensure a suitable and transparent organisational and operational structure for that credit institution and should have a written description of it. The structure should promote and demonstrate the effective and prudent management of an credit institution at individual, sub-consolidated and consolidated levels. The management body should ensure that the internal control functions are independent of the business lines they control, including that there is an adequate segregation of duties, and that they have the appropriate financial and human resources as well as powers to effectively perform their role. The reporting lines and the allocation of responsibilities, in particular among key function holders, within an credit institution should be clear, well-defined, coherent, enforceable and duly documented. The documentation should be updated as appropriate.

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

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

6.2 Know your structure

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

73. The management body should be responsible for the approval of sound strategies and policies for the establishment of new structures. Where an credit 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 credit 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 credit institution's staff, shareholders and other stakeholders and to the competent authority.

74. The management body should guide the credit 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.

75. The management body of a consolidating credit 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 credit 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 credit institutions within the group comply with all supervisory reporting requirements on an individual, sub-consolidated and consolidated basis.

76. The management body of a consolidating credit institution should ensure that the different group entities (including the consolidating credit 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 credit 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 credit 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

77. Credit institutions should avoid setting up complex and potentially non-transparent structures. Credit 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[38]. To this end, credit 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[39];

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 credit institution's management body or the credit institution's ability to manage the related risk; and

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

78. In any case, credit institutions should not set up opaque or unnecessarily complex structures which have no clear economic rationale or legal purpose or if credit institutions are concerned that these structures might be used for a purpose connected with financial crime.

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

80. Credit institutions should document their decisions and be able to justify their decisions to competent authorities.

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

[39] 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

81. 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 credit institution has in place adequate policies and procedures and documented processes (e.g. applicable limits, information requirements) 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 credit 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 credit institution periodically assesses the continuing need to maintain such structures.

82. 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.

83. Credit institutions should take the same risk management measures as for the credit 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, credit institutions should analyse the reason why a client wants to set up a particular structure.

7 Organisational framework in a group context

84. 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 and 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 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[40]. Competent functions within the consolidating credit institution and its subsidiaries should interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms should ensure that the consolidating

[40] Please referalso to the EBA guidelines on sound remuneration policies

credit institution has sufficient data and information and is able to assess the group-wide risk profile, as detailed in Section 6.2.

85. 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.

86. At the consolidated and sub-consolidated levels, the consolidating credit institution should ensure adherence to the group-wide governance policies and internal control framework as referred to in Title V by all credit 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 credit institution should ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

87. A consolidating credit 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.

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

89. The consolidating credit 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.

90. The governance requirements of Directive 2013/36/EU and these guidelines apply to credit 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 credit 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 credit institution should ensure that the group-wide governance policy of the parent credit 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 these guidelines.

91. When establishing policies and documenting governance arrangements, credit institutions should take into account the aspects listed in Annex I to the guidelines. While policies and

documentation may be included in separate documents, credit institutions should consider combining them or referring to them in a single governance framework document.

Question 4: Paragraph 84 and 86 have been amended to reflect changes to CRD. Are those paragraphs sufficiently clear?

Title IV – Risk culture and business conduct

8 Risk culture

92. A sound, righteous and consistent risk culture should be a key element of credit institutions' effective risk management and should enable credit institutions to make sound and informed decisions.

93. Credit institutions should develop an integrated and credit 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 credit institution's risk appetite.

94. Credit institutions should develop a risk culture through policies, communication and staff training regarding the credit 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.

95. 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 credit institution's policies, procedures and controls, taking into account the credit institution's risk appetite and risk capacity.

96. 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 credit institution's core values and expectations. The behaviour of its members should reflect the values. Credit 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 credit institution (e.g. to the competent authority through a whistleblowing process). The management body should on an ongoing basis promote, monitor and assess the risk culture of the credit institution; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the credit institution; and make changes where necessary.

    b. Accountability: relevant staff at all levels should know and understand the core values of the credit 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 credit 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 credit institution's risk profile and its long-term interest[41].

9 Corporate values and code of conduct

97. The management body should develop, adopt, adhere to and promote high ethical and professional standards, taking into account the specific needs and characteristics of the credit 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 credit institution's group-wide standards or common standards released by associations or other relevant organisations.

98. Credit institutions should have policies that ensure that there is no discrimination of staff based on gender, race, colour, ethnic or social origin, genetic features, religion or belief, membership of a national minority, property, birth, disability, age, or sexual orientation.

99. Credit institutions policies should be gender neutral and credit institutions should implement measures that ensure equal opportunities for all genders, including with regard to career perspectives and to improve the representation of the underrepresented gender in management positions.[42]

Question 5: Are paragraphs 98 and 99 sufficiently clear? They have been added to reflect changes in CRD V and to link the Guidelines to Article 157 TFEU and Article 21 of the European Charter of Fundamental Rights.

100. The implemented standards should aim to reduce the risks to which the credit institution is exposed, in particular operational and reputational risks, which can have a considerable adverse impact on an credit institution's profitability and sustainability through fines,

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

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

litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties, and the loss of brand value and consumer confidence.

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

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

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

Question 6: Point (c) of paragraph 101 has been amended to reflect the EBA's work on dividend arbitrage schemes. Is point (c) sufficiently clear?

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

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

102. Credit institutions should monitor compliance with such standards and ensure staff awareness, e.g. by providing training. Credit 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

103. 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 credit institution, of different credit institutions

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

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

105. Credit 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.

106. Actual or potential conflicts of interest that have been identified within the credit institution should be appropriately assessed and managed. If a conflict of interest is identified, the credit 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.

11 Loans and other transactions with members of the management body and their related parties

107. The management body should set out a framework for granting loans and entering into other transactions (e.g. factoring, leasing, property transactions, etc.) with members of the management body and their related parties. Such framework should include limits for loans and transactions (e.g. per product type) and ensure that they are conducted at arm's length. Changes to such limits should require an approval by the management body. The management body should also set out the applicable decision processes for granting such loans and entering into other transactions. This framework may provide for a differentiation between standard business transactions[43] entered into in the ordinary course of business and concluded on normal market terms, staff loans and transactions, which are concluded on conditions available to all staff, and other loans and other transactions that are fair and reasonable from the perspective of the institution and of the shareholders or owners and could also be granted to some third parties. Furthermore, the framework may differentiate between material and non-material loans and other transactions. The framework and decision making process may be different for different types of loans and other transactions,

[43] Business transactions include loans and other transactions (e.g. leasing, factoring, services in the context of IPO, mergers and acquisitions, selling and buying property).

also taking into account their volume and the level of actual or potential conflicts of interest they may create.

108. Decisions on material loans or other material transactions with members of the management body or their related parties that have not been concluded under standard conditions or normal market terms should be made by the management body. The individuals personally concerned by a loan to or other transaction with a member of the management body or their related parties should not be involved in the decision making.

109. Credit institutions should ensure that all relevant internal control procedures fully apply to such loans and other transactions and that an appropriate oversight framework is in place. For non-material loans and other transactions that are concluded on standard conditions or normal market terms as referred to in paragraphs 107 and 108, the management body in its supervisory function should establish an internal procedure to periodically assess whether the conditions for such loans and other transactions are fulfilled. The same should apply, where the decision on a material loan or a material other transaction in line with national law has been taken only by the management body in its management function.

110. When deciding on a loan or other transaction with a member of the management body or their related parties institutions should assess before taking a decision:

a. the risk to which the institution might be exposed due to the transaction; and

b. whether or not the transaction is fair and reasonable from the perspective of the institution and of its shareholders or owners.

111. Where loans are arranged as a line of credit (e.g. overdrafts), the initial decision and amendments thereof should be documented, while any use of such agreed credit facilities within the agreed limits should not be considered as a new decision on a loan to a member of the management body or their related party. Where an amendment of a line of credit is material, a new assessment and decision according to the guidelines in this section should be made.

112. Credit institutions should document data on loans[44] to members of the management body and their related parties properly, including at least:

a. the name of the debtor and his status (i.e. member of the management body or related party) and regarding loans to a related party, the member of the management body concerned and the nature of the link with the related party;

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

c. the terms and conditions applicable to the loan;

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

d. the date of approval of the loan;

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

f. information supporting that the loan was at arm's length, including conditions available to all staff or conditions that are fair and reasonable from the perspective of the institution and of its shareholders or owners (e.g. information on interest rates, fees, commissions, information on comparable loans and transactions with third parties);

g. for loans above an amount of EUR 200 000:

   i. the percentage of the loan and the aggregated exposures towards the same debtor compared to the total eligible capital and common equity Tier-1 capital of the credit institution and whether it is a large exposure[45]; and

   ii. the relative weight of the loan and the aggregated exposures, calculated as percentages by dividing the amount of the approved loan and the aggregated exposures by the total amount of loans to members of the management body and their related parties.

113. Credit institutions should properly document all other material transactions with members of the management body and their related parties taking into account the requirement applicable for the documentation of loans.

114. Credit 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.

115. Credit institutions should make available annually to their shareholders or owners appropriate aggregated information on loans and other transactions with members of the management body and their related parties.

116. Without prejudice to the implementation of Directive 2013/36/EU by member States, credit institutions may consider additional categories of related parties to whom they apply, in whole or in part, this section (e.g. it could be considered, at least, to apply those guidelines to qualified shareholders of the credit institution and the companies on which the credit institution exerts control or significant influence).

[45] See also part IV of Regulation (EU) No 575/2013 and in particular article 392.

Question 7: Section 11 has been added to provide guidelines on loans and transactions with members of the management body and their related parties, reflecting changes to CRD. Is the section appropriate and sufficiently clear?

12 Conflict of interest policy for staff[46]

117. 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 credit 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 credit institution should consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.

118. The policy should aim to identify conflicts of interest of staff, including the interests of their closest family members. Credit 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, credit institutions should assess their materiality and decide on and implement as appropriate mitigating measures.

119. Regarding conflicts of interest that may result from past relationships, credit 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.

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

a. economic interests (e.g. shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the credit 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 credit institution;

c. personal or professional relationships with staff of the credit 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);

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

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.

121. Notwithstanding the above, credit institutions should take into consideration that being a shareholder of an credit institution or having private accounts or loans with or using other services of an credit 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.

122. 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.

123. 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 credit institution should be central to the decisions taken.

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

a. entrusting conflicting activities or transactions to different persons;

b. preventing staff who are also active outside the credit institution from having inappropriate influence within the credit 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 credit institution may be otherwise compromised;

d. preventing members of the management body from holding directorships in competing credit institutions, unless they are within credit institutions that belong to the same credit institutional protection scheme, as referred to in Article 113(7) of Regulation (EU) No 575/2013, credit credit institutions permanently affiliated to a central body, as referred to in Article 10 of Regulation (EU) No 575/2013, or credit institutions within the scope of prudential consolidation.

125. 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 credit institution. Credit institutions should take into consideration that conflicts of interest can have an impact on the independence of mind of members of the management body[47].credit institution

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

127. Actual or potential conflicts of interest that have been disclosed to the responsible function within the credit institution should be appropriately assessed and managed. If a conflict of interest of staff is identified, the credit 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.

128. 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.

Question 8: Paragraph 126 has been added, is it sufficiently clear?

13 Internal alert procedures

129. Credit 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. Credit 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.

130. To avoid conflicts of interest, it should be possible for staff to report breaches outside regular reporting lines (e.g. through the compliance function, the internal audit function or an independent internal whistleblowing procedure). The alert procedures should ensure the protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679[48] (GDPR).

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

[48] 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)

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

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

133. Credit 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 credit institution should ensure that no person under the credit 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.

134. Credit 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 credit 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.

135. In particular, internal alert procedures should:

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

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

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

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

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

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

g. ensure appropriate record keeping.

14 Reporting of breaches to competent authorities

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

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

b. appropriate protection as referred to in Section 13;

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

d. clear procedures as set out in paragraph 135.

137. 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 credit institutions' internal alert procedures.

Title V – Internal control framework and mechanisms

15 Internal control framework

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

139. The internal control framework of the credit institution concerned 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. The credit institutions concerned must organise the exchange of the information necessary 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, AML/CFT compliance function where different,

at the group level and between the heads of the internal control functions at the group level and the management body of the credit institution.

140. Credit 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. Credit institutions should assess their exposure to the risk that they may be used for the purpose of ML/TF and take mitigating measures to reduce those risks as well as their operational and reputational risks linked to them. Credit 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 credit institution and the integrity of the financial system.

Question 9: Paragraph 140 has been added, is it sufficiently clear?

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

142. The internal control framework of an credit 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 credit institution's internal policies, processes, rules and decisions.

16 Implementing an internal control framework

143. 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, i AML/CFT compliance where different from the compliance function, and internal audit functions). Credit institutions should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures, which should be approved by the management body.

144. An credit 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.

145. Credit institutions should communicate those policies, mechanisms and procedures to all staff and every time material changes have been made.

146. When implementing the internal control framework, credit 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.

147. 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.

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

17 Risk management framework

149. As part of the overall internal control framework, credit institutions should have a holistic credit 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 credit 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 credit 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 credit institution and at consolidated or sub-consolidated level. All relevant risks should be encompassed in the risk management framework with appropriate consideration of both financial and non-financial risks, including credit, market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance ML/FT and other financial crime, ESG, and strategic risks.

150. An credit 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, credit institution and consolidated or sub-consolidated levels.

151. An credit 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 credit institution's risk appetite and commensurate with its sound operation, financial strength, capital base and strategic goals. An credit 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.

152. The risk management framework should be subject to independent internal review, e.g. performed by the internal audit function, and reassessed regularly against the credit 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 credit institution's business, risk profile or operating structure; geographic expansion; mergers and acquisitions; and the introduction of new products or business lines.

153. When identifying and measuring or assessing risks, an credit 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 credit 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 credit institution's risk capacity. The tools should provide information on any adjustment to the risk profile that may be required. Credit institutions should make appropriately conservative assumptions when building stressed scenarios.

154. Credit 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 credit 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.

155. The ultimate responsibility for risk assessment lies solely with the credit institution, which, accordingly, should evaluate its risks critically and should not rely exclusively on external

assessments. For example, an credit 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.

156. Credit 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).

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

158. Regular and transparent reporting mechanisms should be established so that the management body, its risk committee, where established, and all relevant units in an credit 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.

159. 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 credit institution and up and down the management chain.

18 New products and significant changes[49]

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

161. 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

[49] 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.

purpose vehicles; new products; changes to systems or the risk management framework or procedures; and changes to the credit institution's organisation.

162. An credit 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.

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

164. 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 their obligations under Directive (EU) 2015/849, credit 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.

165. 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 credit institution's risk management and internal control frameworks, and of the ability of the credit institution to manage any new risks effectively. The risk management function should also have a clear overview of the roll-out of new products (or significant changes to existing products, processes and systems) across different business lines and portfolios, and the power to require that changes to existing products go through the formal NPAP process.

19 Internal control functions

166. The internal control functions should include a risk management function (see Section 20), a compliance function (see Section 21) and an internal audit function (see Section 22). The risk management and compliance functions should be subject to review by the internal audit function. The responsibilities of control functions also include to ensure compliance with AML/TF requirements.

167. The operational tasks of the internal control functions may be outsourced, taking into account the proportionality criteria listed in Title I, to the consolidating credit institution or another entity within or outside of the group with the consent of the management bodies of the credit institutions concerned. Even when internal control operational tasks are partially or fully outsourced, 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 credit institution.

19.1 Heads of the internal control functions

168. Heads of internal control functions should be established at an adequate hierarchical level that provides the head of the control function with the appropriate authority and stature needed to fulfil his or her responsibilities. Notwithstanding the overall responsibility of the management body, heads of internal control functions should be independent of the business lines or units they control. To this end, the heads of the risk management, compliance and internal audit functions should report and be directly accountable to the management body, and their performance should be reviewed by the management body.

169. Where necessary, the heads of internal control functions should be able to have access and report directly to the management body in its supervisory function to raise concerns and warn the supervisory function, where appropriate, when specific developments affect or may affect the credit institution. This should not prevent the heads of internal control functions from reporting within the regular reporting lines as well.

170. Credit institutions should have documented processes in place to assign the position of the head of an internal control function and for withdrawing his or her responsibilities. In any case, the heads of internal control functions should – and under Article 76(5) of Directive 2013/36/EU the head of the risk management function must – not be removed without the prior approval of the management body in its supervisory function. In significant credit institutions, competent authorities should be promptly informed about the approval and the main reasons for the removal of a head of an internal control function.

19.2 Independence of internal control functions

171. In order for the internal control functions to be regarded as independent, 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 credit 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 not otherwise likely to compromise their objectivity[50].

19.3 Combination of internal control functions

172. Taking into account the proportionality criteria set out in Title I, the risk management function and compliance function may be combined. The internal audit function should not be combined with another internal control function.

19.4 Resources of internal control functions

173. 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.

174. Internal control functions should have appropriate IT 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 credit institutiones.

20 Risk management function

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

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

177. 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.

[50] 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.

178. 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.

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

180. The RMF should be a central organisational feature of the credit 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 credit institution has effective risk management processes in place. The RMF should be actively involved in all material risk management decisions.

181. Significant credit 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 credit institution, to deliver an credit institution- and group-wide holistic view on all risks and to ensure that the risk strategy is complied with.

182. 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 credit institution's risk appetite and strategy. The RMF may recommend improvements to the risk management framework and corrective measures to remedy breaches of risk policies, procedures and limits.

20.1 RMF's role in risk strategy and decisions

183. The RMF should be actively involved at an early stage in elaborating an credit institution's risk strategy and in ensuring that the credit institution has effective risk management processes in place. The RMF should provide the management body with all relevant risk-related information to enable it to set the credit 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 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. Targets should be plausible and consistent with the credit institutions risk strategy.

184. 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.

20.2 RMF's role in material changes

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

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

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

187. The RMF should ensure that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the credit institution.

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

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

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

191. The RMF should regularly monitor the actual risk profile of the credit institution and scrutinise it against the credit institution's strategic goals and risk appetite to enable decision-making by the management body in its management function and challenge by the management body in its supervisory function.

192. 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.

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

20.4 RMF's role in unapproved exposures

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

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

20.5 Head of the risk management function

196. 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 credit institution's overall risk profile. The same applies to the head of the RMF of a parent credit institution regarding the consolidated situation.

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

198. The head of the RMF should be able to challenge decisions taken by the credit institution's management and its management body, and the grounds for objections should be formally documented. If an credit 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.

199. Credit 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 credit institution's risk appetite and strategy.

21 Compliance function

200. Credit institutions should establish a permanent and effective compliance function to manage compliance risk, and should appoint a person to be responsible for this function across the entire credit institution (the compliance officer or head of compliance).

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

202. The compliance function, including the head of compliance, should be independent of the business lines and internal units it controls and have sufficient authority, stature and resources. Taking into account the proportionality criteria set out in Title I, this function may be assisted by the RMF or combined with the RMF or other appropriate functions, e.g. the legal division or human resources.

203. 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.

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

205. 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 credit institution’s activities and compliance framework.

206. 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 credit institution’s compliance risk 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.

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

208. Credit 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).

209. Credit 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 credit institution.

22 Internal audit function

210. Credit 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 credit institution. The IAF should be independent and have sufficient authority, stature and resources. In particular, the credit 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 credit institution's size and locations, and the nature, scale and complexity of the risks associated with the credit institution's business model, activities, risk culture and risk appetite.

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

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

213. 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.

214. The IAF should assess whether the credit institution's internal control framework as set out in Section 15 is both effective and efficient. In particular, the IAF should assess:

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

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

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

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

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

215. The IAF should verify, in particular, the integrity of the processes ensuring the reliability of the credit 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.

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

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

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

219. 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.

220. 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[51]

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

221. Credit institutions should establish a sound business continuity management and recovery plan to ensure their ability to operate on an ongoing basis and to limit losses in the event of severe business disruption.

222. Credit institutions may establish a specific independent business continuity function, e.g. as part of the RMF[52].

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

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

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

a. contingency and business continuity plans to ensure that the credit institution reacts appropriately to emergencies and is able to maintain its most important business activities if there is disruption to its ordinary business procedures; and

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

226. Contingency, business continuity and recovery plans should be documented and carefully implemented. The documentation should be available within the business lines, internal units and RMF, and should be stored on systems that are physically separated and readily accessible in case of contingency. Appropriate training should be provided. Plans should be regularly tested and updated. Any challenges or failures occurring in the tests should be documented and analysed, with the plans reviewed accordingly.

[52] Please refer also to Article 312 of Regulation (EU) No 575/2013.

Title VII – Transparency

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

228. Accordingly, the management body should inform and update the relevant staff about the credit 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.

229. 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 credit institutions, the information should include all entities within the group structure as defined in Directive 2013/34/EU[53], by country.

230. The publication should include at least:

a. an overview of the internal organisation of the credit 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 credit institutions and to the management body;

h. an overview of the internal control framework; and

[53] 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).

i. an overview of the business continuity management framework.

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

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

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

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

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. The EBA Guidelines on internal Governance needed to be amended to reflect those changes and to align their wording with other EBA work.

3. The amendments to the Guidelines should ensure that credit institutions have specific governance arrangements regarding the management of money laundering and terrorist financing risks and to avoid that they contribute to dividend arbitrage schemes. Credit institutions should also have a strong framework to manage conflicts of interests and ensure prudent decision making in the context of loans to related parties.

C. Baseline scenario

4. The current EU legislative framework for credit institutions' internal governance consists mainly of Directive 2013/36/EU, 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 outsourcing.

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

D. Options considered

6. The section on outsourcing has been removed as the EBA has issued Guidelines on Outsourcing. This change has no further impact.

7. Guidelines have been provided on the code of conduct that link the Guidelines to the requirements on non-discrimination and equal opportunities within the European Charter of Fundamental Rights and the Treaty on the Functioning of the European Union. Those additions have no impact as the underlying provisions apply based on the aforementioned frameworks.The guidelines provide additional clarity about the governance requirements in the context of AML/CTF provisions. Credit institutions should already have sufficient governance arrangements in place to ensure that they comply with Anti Money Laundering, Anti Terrorist Financing and tax laws. The related risks are already covered by the requirement on institutions to manage all their risks. Hence, the clarifications provided in the guidelines should not trigger any implementation costs if the credit institution concerned had already the required arrangementds in place and had implemented the requirements under Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015.

8. In addition the Guidelines have been clarified regarding the management of conflicts of interest in relation to loans and other transactions to members of the management body and their related parties. Given that specific provisions have been added to Directive 2013/36/EU it was considered necessary to clarify the regulatory expections and the requirements with regard to the documentation of such loans and the management of related conflicts of interest. The objective of the changes are that there is sufficient scrutiny on decision regarding such loans and that conflicts of interest in that context are appropriately managed. Restricting the Guidelines to loans to members of the management body and their related parties would not be effective as also other transaction might create material conflicts of interests. It is necessary to require a documentation of such transactions. In any case it is required that credit institutions document all transactions. However, minor additional costs are created, caused by specific additional documentation requirements, which are necessary to ensure that the impact of such transactions and the conflicts of interest they potentially create can be assessed by institutions and competent authorities.

9. The guidelines have been shaped to be consistent with the requirements set out in this Shareholders Rights Directive. In line with the principle of proportionality the guidelines differentiate between requirements for material and non material loans and transactions. The requirements specify the already existing requirements for all institutions. For institutions that are not subject to the Shareholder Rights Directive minor implementation costs may be triggered as an adjustment to their conflict of interest framework may be necessary.

E. Cost-benefit analysis

10. Given the limited amendments to the guidelines and given that they are based on amendments of Directive 2013/36/EU and other existing legal requirements, it is assumed

that the changes to the Guidelines as such create no or if at all very low implementation costs for updates to internal policies and additional required documentations.

5.2. Questions for public consultation

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

Question 2: Point (d) has been added, throughout the Guidelines references to money laundering and terrorism financing and the institutions obligations have been added, are those references sufficiently clear?

Question 3: Paragraph 24 regarding ESG factors has been added, is it sufficiently clear?

Question 4: Paragraph 84 and 86 have been amended to reflect changes to CRD. Are those paragraphs sufficiently clear?

Question 5: Are Paragraphs 98 and 99 sufficiently clear?

Question 6: Point (c) of paragraph 101 has been amended to reflect the EBA's work on dividend arbitrage schemes. Is point (c) sufficiently clear?

Question 7: Section 11 has been added to provide guidelines on loans and transactions with members of the management body and their related parties, reflecting changes to CRD. Is the section appropriate and sufficiently clear?

Question 8: Paragraph 126 has been added, is it sufficiently clear?

Question 9: Paragraph 140 has been added, is it sufficiently clear?