EBA/GL/2017/11

26 September 2017

Final Report

Guidelines

on internal governance under Directive 2013/36/EU

Contents

Executive Summary

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

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

To further harmonise 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 of Directive 2013/36/EU to develop guidelines in this area. The guidelines apply to all institutions regardless of their governance structures (unitary board, dual board or other structure), without advocating or preferring any specific structure, as set out specifically in the scope of application. 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 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 institution's activities and to strengthen the risk management frameworks of institutions. Additional guidelines have been provided to further increase the transparency of institutions' offshore activities and to ensure the consideration of risks within institutions' change processes.

Next steps

The EBA has published its guidelines on internal governance, which will enter into force on 30 June 2018. The existing guidelines on internal governance, published on 27 September 2011, will be repealed at the same time. On the same date, the EBA and ESMA joint guidelines on the assessment of the suitability of members of the management body and key function holders will come into force.

Background and rationale

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

2. In recent years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct institutions' weak or superficial internal governance practices, as identified during the financial crisis. 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 institutions resulted in a lack of effective oversight of management decision-making, which led to short-term oriented and excessively risky management strategies. Weak oversight by the management body in its supervisory function has been identified as a contributing factor. The management body, both in its management function and, in particular, in its supervisory function, might not have understood the complexity of the business and the risks involved, consequently failing to identify and constrain excessive risk-taking in an effective manner.

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

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

6. Against this background, there is a clear need to address 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 institutions and to enable competent authorities to supervise and monitor the adequacy of internal governance arrangements.

Legal basis

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

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

9. 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 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 remembered that business lines or units, as the first line of defence, have a material role in ensuring robust risk management and compliance within an institution.

10. 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 institutions.

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

12. Article 109(2) of Directive 2013/36/EU requires parent undertakings and subsidiaries subject to this Directive to meet the governance requirements also on a consolidated or sub-consolidated basis, to ensure that their arrangements, processes and mechanisms are consistent and well-integrated and that any data and information relevant to the purpose of supervision can be produced. 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. 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.

13. 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 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.

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

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

16. The guidelines should be read in conjunction with and without prejudice to the guidelines on sound remuneration policies (EBA/GL/2015/22) and the joint guidelines on the assessment of the suitability of members of the management body and key function holders. The existing guidelines on internal governance, published on 27 September 2011, will be repealed when the new guidelines enter into force.

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

Rationale and objective of the guidelines

18. Internal governance includes all standards and principles concerned with setting an institution's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined 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.

19. 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.

20. In addition, it is also necessary to take into account developments in this area since the publication of the EBA guidelines on internal governance in 2011, such as the updated OECD principles of corporate governance[1] and the revised corporate governance principles for banks published by the Basel Committee on Banking Supervision (BCBS)[2]. 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) (EBA/GL/2014/13) 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 institution is willing to assume, while 'risk capacity' is the maximum amount of risk an institution is able to assume.

21. 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.

22. 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.

23. 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 institution's governing body or bodies under national law.

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

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

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

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

25. 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.

26. 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[3].

27. 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 institutions. To take into account the principle of proportionality, simpler requirements have been introduced for smaller institutions.

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

29. 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 institution's risk appetite and that the business activities are in compliance with external and internal requirements.

30. 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 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

[3] 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.

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.

31. 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.

32. 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.

33. 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 institution's size, internal organisation and nature, and the complexity of its activities.

34. 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 institutions on governance arrangements, including in relation to such structures.

35. The guidelines aim to establish a sound risk culture in institutions. Risks should be taken within a well-defined framework in line with the institution's risk strategy and appetite. This includes the establishment of and ensuring compliance with a system of limits and controls. Risks within new products and business areas, but also risks that may result from changes to institutions' products, processes and systems, are to be duly identified, assessed, appropriately managed and monitored. The risk management function and compliance function should be involved in the establishment of the framework and the approval of such changes to ensure that all material risks are taken into account and that the institution complies with all internal and external requirements.

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

EBA/GL/2017/11

DD Month YYYY

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[4]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authority and financial institutions must make every effort to comply with the guidelines.

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

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authority must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authority will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2017/11'. 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.

[4] 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 and investment firms must implement in accordance with Article 74(1) of Directive 2013/36/EU[5] to ensure effective and prudent management of the 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[6], including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013, and to institutions as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013.

Scope of application

7. These guidelines apply in relation to institutions' governance arrangements, including their organisational structure and the corresponding lines of responsibility, processes to identify, manage, monitor and report the risks they are or might be exposed to, and internal control framework.

8. The guidelines intend to embrace all existing board structures and do not advocate any particular structure. The guidelines do not interfere with the general allocation of competences in accordance with national company law. Accordingly, they should be applied 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[7].

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

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

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

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

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 institution's governing body or bodies under national law.

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

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

Definitions

14. Unless otherwise specified, terms used and defined in Directive 2013/36/EU have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

Risk appetite	means the aggregate level and types of risk an institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.
Risk capacity	means the maximum level of risk an institution is able to assume given its capital base, its risk management and control capabilities, and its regulatory constraints.
Risk culture	means an institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day

	activities and has an impact on the risks they assume.
Institutions	means credit institutions and investment firms as defined in Article 4(1)(1) and (2), respectively, of Regulation (EU) No 575/2013.
Staff	means all employees of an institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to Directive 2013/36/EU, and all members of the management body in its management function and in its supervisory function.
Chief executive officer (CEO)	means the person who is responsible for managing and steering the overall business activities of an institution.
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 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 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. Prudential consolidation includes all subsidiaries that are institutions or financial institutions, as defined in Article 4(3) and (26), respectively, of Regulation (EU) No 575/2013, and may also include ancillary services undertakings, as defined in Article 2(18) of that Regulation, established in and outside the EU.
Consolidating institution	means an institution that is required to abide by the prudential requirements on the basis of the consolidated situation in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013.

Significant institutions	means institutions referred to in Article 131 of Directive 2013/36/EU (global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs)), and, as appropriate, other institutions determined by the competent authority or national law, based on an assessment of the institutions' size and internal organisation, and the nature, scope and complexity of their activities.
Listed CRD-institution	means institutions whose financial instruments are admitted to trading on a regulated market or on a multilateral trading facility as defined under Article 4, paragraphs (21) and (22) of Directive 2014/65/EU, in one or more Member States[8].
Shareholder	means a person who owns shares in an institution or, depending on the legal form of an institution, other owners or members of the institution.
Directorship	means a position as a member of the management body of an institution or another legal entity.

3. Implementation

Date of application

15. These guidelines apply from 30 June 2018.

Repeal

16. The EBA guidelines on internal governance (GL 44) of 27 September 2011 are repealed with effect from 30 June 2018.

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

4. Guidelines

Title I – Proportionality

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

18. Institutions should take into account their size and internal organisation, and the nature, scale and complexity of their activities, when developing and implementing internal governance arrangements. Significant institutions should have more sophisticated governance arrangements, while small and less complex institutions may implement simpler governance arrangements.

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 institutions and competent authorities:

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

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

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

    d. whether the institution is listed or not;

    e. whether the institution is authorised to use internal models for the measurement of capital requirements (e.g. the Internal Ratings Based Approach);

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

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

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

i. the ownership and funding structure of the institution;

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

k. the outsourced activities and distribution channels; and

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

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

1 Role and responsibilities of the management body

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

21. 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.

22. 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. 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. 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.

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

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

b. the overall risk strategy, including the 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. the amounts, types and distribution of both internal capital and regulatory capital to adequately cover the risks of the institution;

e. targets for the liquidity management of the institution;

f. a 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[9];

g. arrangements aimed at ensuring that the individual and collective suitability assessments of the management body are carried out effectively, that the composition and succession planning of the management body are appropriate, and that the management body performs its functions effectively[10];

h. a selection and suitability assessment process for key function holders[11];

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

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

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

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

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

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

[9] 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).

[10] 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.

[11] See also 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.

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

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

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

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

27. The management body should monitor, periodically review and address any weaknesses identified regarding the implementation of processes, strategies and policies related to the responsibilities listed in paragraphs 23 and 24. The internal governance framework and its implementation should be reviewed and updated on a periodic basis taking into account the proportionality principle, as further explained in Title I. A deeper review should be carried out where material changes affect the institution.

2 Management function of the management body

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

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

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

3 Supervisory function of the management body

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

32. 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.

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

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

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

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

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

    e. oversee and monitor that the institution's strategic objectives, organisational structure and risk strategy, 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 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 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

34. 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.

35. 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.

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

37. 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.

38. 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

39. In accordance with Article 109(1) of Directive 2013/36/EU in conjunction with Articles 76(3), 88(2), and 95(1) of Directive 2013/36/EU, all institutions that are themselves significant, considering the individual, sub-consolidated and consolidated levels, must establish risk, nomination [12] and remuneration [13] committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this body. Non-significant institutions, including when they are within the scope of prudential consolidation of an institution that is significant in a sub-consolidated or consolidated situation, are not obliged to establish those committees.

40. 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.

41. Institutions may, taking into account the criteria set out in Title I of these guidelines, establish other committees (e.g. ethics, conduct and compliance committees).

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

43. 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.

44. 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[14]

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

46. Independent members[15] of the management body in its supervisory function should be actively involved in committees.

47. 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.

[12] 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.

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

[14] 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.

[15] 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.

48. 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.

49. 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.

50. The risk and nomination committees should be composed of non-executive members of the management body in its supervisory function of the institution concerned. The audit committee should be composed in accordance with Article 41 of Directive 2006/43/EC[16]. The remuneration committee should be composed in accordance with Section 2.4.1 of the EBA guidelines on sound remuneration policies[17].

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

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

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

54. 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

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

[16] 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.

[17] 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).

56. Committees should interact with each other as appropriate. Without prejudice to paragraph 48, 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.

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

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

59. The risk and nomination committees should at least:

    a. have access to all relevant information and data necessary to perform their role, including information and data from relevant corporate and control functions (e.g. legal, finance, human resources, IT, risk, 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 institution, its risk culture and its risk limits, as well as on any material breaches that may have occurred, with detailed information on and recommendations for corrective measures taken, to be taken or suggested to address them;

    c. periodically review and decide on the content, format and frequency of the information on risk to be reported to them; and

    d. 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

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

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

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

    c. oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of an institution, such as market, credit, operational (including legal and IT 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 institution, market developments or recommendations made by the risk management function;

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

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

g. oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the institution[18]. 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.

61. The risk committee should collaborate with other committees whose activities may have an impact on the risk strategy (e.g. audit and remuneration committees) and regularly communicate with the institution's internal control functions, in particular the risk management function.

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

5.5 Role of the audit committee

63. In accordance with Directive 2006/43/EC[19], where established, the audit committee should, inter alia:

[18] 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.

[19] 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.

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

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

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

d. review and monitor the independence of the statutory auditors or the audit firms in accordance with Articles 22, 22a, 22b, 24a and 24b of Directive 2006/43/EU and Article 6 of Regulation (EU) No 537/2014[20], and in particular the appropriateness of the provision of non-audit services to the audited institution in accordance with Article 5 of that Regulation;

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

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

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

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

i. receive and take into account audit reports.

5.6 Combined committees

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

[20] 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).

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

66. 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[21].

Title III – Governance framework

6 Organisational framework and structure

6.1 Organisational framework

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

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

69. 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 institution's organisational framework. Where weaknesses are identified, the management body should make any necessary adjustments swiftly.

6.2 Know your structure

[21] 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.

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

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

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

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

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

    a. information on major risk drivers;

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

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

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

75. Institutions should avoid setting up complex and potentially non-transparent structures. Institutions should take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with money laundering or other financial crimes and the respective controls and legal framework in place[22]. To this end, institutions should take into account at least:

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

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

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

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

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

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

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

77. 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

[22] For further details on the assessment of country risk and the risk associated with individual products and customers, institutions should refer also to the final (once issued) joint guidelines on risk factors: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper .

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.

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

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

    a. the institution has in place adequate policies and procedures and documented processes (e.g. applicable limits, information 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 institution and internal and external auditors and is reported to the management body in its supervisory function and to the competent authority that granted authorisation; and

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

80. 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.

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

7 Organisational framework in a group context

82. 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 to ensure robust governance arrangements on a consolidated and sub-consolidated basis. Competent functions within the consolidating institution and its subsidiaries should interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms should ensure that the consolidating institution has sufficient data and information and is able to assess the group-wide risk profile, as detailed in Section 6.2.

83. 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.

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

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

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

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

88. The governance requirements of Directive 2013/36/EU and these guidelines apply to institutions independent of the fact that they may be subsidiaries of a parent undertaking in a third country. Where an EU subsidiary of a parent undertaking in a third country is a consolidating institution, the scope of prudential consolidation does not include the level of the parent undertaking located in a third country and other direct subsidiaries of that parent undertaking. The consolidating institution should ensure that the group-wide governance policy of the parent institution in a third country is taken into consideration within its own

governance policy insofar as this is not contrary to the requirements set out under relevant EU law, including Directive 2013/36/EU and these guidelines.

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

8 Outsourcing policy[23]

90. The management body should approve and regularly review and update the outsourcing policy of an institution, ensuring that appropriate changes are implemented in a timely manner.

91. The outsourcing policy should consider the impact of outsourcing on an institution's business and the risks it faces (such as operational risks, including legal and IT risks; reputational risks; and concentration risks). The policy should include the reporting and monitoring arrangements to be implemented from inception to the end of an outsourcing agreement (including drawing up the business case for outsourcing, entering into an outsourcing contract, the implementation of the contract to its expiry, contingency plans and exit strategies). An institution remains fully responsible for all outsourced services and activities and management decisions arising from them. Accordingly, the outsourcing policy should make it clear that outsourcing does not relieve the institution of its regulatory obligations and its responsibilities to its customers.

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

93. The policy should require that, when selecting material external services providers or when outsourcing activities, the institution must take into account whether or not the service provider has in place appropriate ethical standards or a code of conduct.

Title IV – Risk culture and business conduct

9 Risk culture

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

[23] The present guidelines are limited to the general outsourcing policy; specific aspects of the issue of outsourcing are dealt with in the CEBS guidelines on outsourcing, which are due to be revised. These guidelines are available at https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

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

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

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

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

    a. Tone from the top: the management body should be responsible for setting and communicating the institution's core values and expectations. The behaviour of its members should reflect the values being espoused. Institutions' management, including key function holders, should contribute to the internal communication of core values and expectations to staff. Staff should act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance within or outside the institution (e.g. to the competent authority through a whistleblowing process). The management body should on an ongoing basis promote, monitor and assess the risk culture of the institution; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the institution; and make changes where necessary.

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

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

d. Incentives: appropriate incentives should play a key role in aligning risk-taking behaviour with the institution's risk profile and its long-term interest[24].

10 Corporate values and code of conduct

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

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

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 institution's activities should be conducted in compliance with the applicable law and with the institution's corporate values;

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

c. set out principles on and provide examples of acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, economic and financial crime (including fraud, money laundering and anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws);

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

[24] 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.

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

11 Conflict of interest policy at institutional level

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

104. 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. 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; and

c. establishing adequate procedures for transactions with related parties, e.g. requiring transactions to be conducted at arm's length.

12 Conflict of interest policy for staff[25]

106. The management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and

[25] 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.

mitigate or prevent actual and potential conflicts between the interests of the institution and the private interests of staff, including members of the management body, which could adversely influence the performance of their duties and responsibilities. A consolidating institution should consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.

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

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

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

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

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

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

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

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

f. political influence or political relationships.

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

111. 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.

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

113. 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 institution from having inappropriate influence within the institution regarding those other activities;

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

d. establishing adequate procedures for transactions with related parties (institutions may consider, inter alia, requiring transactions to be conducted at arm's length, requiring that all relevant internal control procedures fully apply to such transactions, requiring binding consultative advice from independent members of the management body, requiring the approval by shareholders of the most relevant transactions and limiting exposure to such transactions); and

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

114. The policy should specifically cover the risk of conflicts of interest at the level of the management body and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of members of the management body to take objective and impartial decisions that aim to fulfil the best interests of the institution.

Institutions should take into consideration that conflicts of interest can have an impact on the independence of mind of members of the management body[26].

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

116. 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.

13 Internal alert procedures

117. 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.

118. 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 Directive 95/46/EC.

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

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

121. Institutions should ensure that the person reporting the breach is appropriately protected from any negative impact, e.g. retaliation, discrimination or other types of unfair treatment. The institution should ensure that no person under the institution's control engages in

[26] 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.

victimisation of a person who has reported a breach and should take appropriate measures against those responsible for any such victimisation.

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

123. 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 Directive 95/46/EC, 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

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

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

b. appropriate protection as referred to in Section 13;

c. protection of the personal data of both the natural person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Directive 95/46/EC; and

d. clear procedures as set out in paragraph 123.

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

Title V – Internal control framework and mechanisms

15 Internal control framework

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

127. The internal control framework of the 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 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 at the group level and between the heads of the internal control functions at the group level and the management body of the institution.

128. 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.

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

a. effective and efficient operations;

b. prudent conduct of business;

c. adequate identification, measurement and mitigation of risks;

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

e. sound administrative and accounting procedures; and

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

16 Implementing an internal control framework

130. 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 and internal audit functions). Institutions should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures, which should be approved by the management body.

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

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

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

134. 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.

135. 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

136. As part of the overall internal control framework, institutions should have a holistic institution-wide risk management framework extending across all its business lines and internal units, including internal control functions, recognising fully the economic substance of all its risk exposures. The risk management framework should enable the institution to make fully informed decisions on risk-taking. The risk management framework should encompass on- and off-balance-sheet risks as well as actual risks and future risks that the institution may be exposed to. Risks should be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the institution and at consolidated or sub-consolidated level. All relevant risks should be encompassed in the risk management framework with appropriate consideration of both financial and non-financial risks, including credit, market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance and strategic risks.

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

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

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

140. When identifying and measuring or assessing risks, an institution should develop appropriate methodologies including both forward-looking and backward-looking tools. The methodologies should allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations. The tools should include the assessment of the actual risk profile against the institution's risk appetite, as well as the identification and assessment of potential and stressed risk exposures under a range of assumed adverse circumstances against the institution's risk capacity. The tools should provide information on

any adjustment to the risk profile that may be required. Institutions should make appropriately conservative assumptions when building stressed scenarios.

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

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

143. 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).

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

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

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

18 New products and significant changes[27]

147. An institution should have in place a well-documented new product approval policy (NPAP), approved by the management body, that addresses the development of new markets, products and services, and significant changes to existing ones, as well as exceptional transactions. The policy should in addition encompass material changes to related processes (e.g. new outsourcing 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 institution and the corresponding limits, or that necessary revisions are made.

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

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

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

151. 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. 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.

152. The risk management function and the compliance function should be involved in approving new products or significant changes to existing products, processes and systems. Their input should include a full and objective assessment of risks arising from new activities under a variety of scenarios, of any potential shortcomings in the institution's risk

[27] 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.

management and internal control frameworks, and of the ability of the 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

153. 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.

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

19.1 Heads of the internal control functions

155. 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.

156. 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 institution. This should not prevent the heads of internal control functions from reporting within the regular reporting lines as well.

157. 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 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

158. 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 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[28].

19.3 Combination of internal control functions

159. 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

160. 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.

161. 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 institutiones.

20 Risk management function

[28] 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.

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

163. 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.

164. 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.

165. 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.

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

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

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

169. The RMF should provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by business lines or internal units, and should inform the management body as to whether they are consistent with the institution's risk 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

170. The RMF should be actively involved at an early stage in elaborating an institution's risk strategy and in ensuring that the 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 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 institutions risk strategy.

171. 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

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

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

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

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

175. 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.

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

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

178. The RMF should regularly monitor the actual risk profile of the institution and scrutinise it against the 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.

179. 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.

180. 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

181. 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.

182. 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

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

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

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

the management body, it should specify the scope of such a veto right, the escalation or appeal procedures, and how the management body will be involved.

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

21 Compliance function

187. 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 institution (the compliance officer or head of compliance).

188. 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.

189. 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.

190. 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.

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

192. The compliance function should advise the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and should assess the possible impact of any changes in the legal or regulatory environment on the institution's activities and compliance framework.

193. The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that the compliance policy is observed. The compliance function should report to the management body and communicate as appropriate with the RMF on the institution's 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.

194. 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.

195. Institutions should take appropriate action against internal or external fraudulent behaviour and breaches of discipline (e.g. breaches of internal procedures, breaches of limits).

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

22 Internal audit function

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

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

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

200. 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.

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

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

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

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

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

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

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

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

204. 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.

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

206. 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.

207. 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

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

209. Institutions may establish a specific independent business continuity function, e.g. as part of the RMF[29].

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

211. In order to establish a sound business continuity management plan, an institution should carefully analyse 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 institution's recovery priorities and objectives.

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

a. contingency and business continuity plans to ensure that the 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 institution to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions should be consistent with the institution's risk appetite.

213. 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.

Title VII – Transparency

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

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

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

216. Where parent undertakings are required by competent authorities under Article 106(2) of Directive 2013/36/EU to publish annually a description of their legal structure and governance and the organisational structure of the group of institutions, the information should include all entities within the group structure as defined in Directive 2013/34/EU[30], by country.

217. The publication should include at least:

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

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

c. new legal, governance or organisational structures;

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

e. the key responsibilities of the management body;

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

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

h. an overview of the internal control framework; and

i. an overview of the business continuity management framework.

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

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

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

1. Shareholder structure
2. Group structure, if applicable (legal and functional structure)
3. Composition and functioning of the management body
   a) selection criteria
   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

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

3. Weaknesses in corporate governance in a number of institutions have contributed to excessive and imprudent risk-taking in the financial sector, which has led to the failure of individual institutions and systemic problems in Member States and globally. The very general provisions on governance of institutions and the non-binding nature of a substantial part of the corporate governance framework, based essentially on voluntary codes of conduct, did not sufficiently facilitate the effective implementation of sound corporate governance practices by institutions. In some cases, the absence of effective checks and balances within institutions resulted in a lack of effective oversight of management decision-making, which exacerbated short-term and excessively risky management strategies.

4. In order to address the potentially detrimental effect of poorly designed corporate governance arrangements on the sound management of risk, requirements to ensure effective oversight by the management body, promote a sound risk culture at all levels of credit institutions and investment firms, and enable competent authorities to monitor the adequacy of internal governance arrangements are needed.

5. Guidelines should ensure that the additional requirements for institutions' internal governance and with regard to the responsibilities of members of the management body introduced by Directive 2013/36/EU are applied in a harmonised way.

B. Policy objectives

6. The EBA has updated the previously issued EBA guidelines on internal governance. The underlying reasons are mainly additions made in Directive 2013/36/EU to the existing regulatory framework. The guidelines were also restructured to increase their clarity and their consistency with other guidelines issued by the EBA in the meantime, in particular with regard to the reinforcement of the requirements regarding risk oversight by the management body and the risk management function, the application of the internal governance arrangements at group level and more precise criteria regarding the application of the proportionality principle.

7. The governance requirements should be applied on a consolidated basis, that is at the levels of the group, parent undertakings and subsidiaries, including branches and subsidiaries established in third countries and subsidiaries to which Directive 2013/36/EU does not directly apply on an individual level.

8. The implementation of internal governance arrangements should reflect differences between types of institutions in a proportionate manner, taking into account their size and internal organisation and the nature, scope and complexity of their activities.

9. In order to ensure a well-functioning internal market, transparent, predictable and harmonised supervisory practices and decisions are necessary for conducting business. The EBA should therefore seek to further harmonise supervisory practices.

10. The EBA aims for the maximum possible harmonisation as a means to achieve a level playing field, prevent regulatory arbitrage opportunities, increase supervisory convergence and achieve legal certainty. In addition, the development of common procedures and practices is expected to reduce the compliance burden on institutions and contribute to efficient and effective cooperation among competent authorities.

11. The EBA has updated the aforementioned guidelines on internal governance in line with the mandate given under Article 74 of Directive 2013/36/EU and based on the reinforced internal governance requirements introduced under this Directive to achieve a higher level of harmonisation, to ensure effective oversight by the management body and to promote a sound risk culture at all levels of credit institutions and investment firms.

12. In particular, the guidelines specify:

    a. the involvement of the management body in the definition and implementation of the governance arrangements, particularly with regard to risk oversight, including through the setting up of specialised committees;

    b. how internal policies are to be applied in a group context;

c. how the principle of proportionality is to be applied by both competent authorities and institutions; and

d. how the internal control framework should be implemented, including how the internal control functions should be organised.

C. Baseline scenario

13. The current EU legislative framework for institutions' internal governance consists mainly of Directive 2013/36/EU; the EBA guidelines on internal governance, published in 2011; the EBA guidelines for common procedures and methodologies for the supervisory review and evaluation process (SREP); the EBA guidelines on sound remuneration policies; and the EBA guidelines on the assessment of the suitability of members of the management body and key function holders.

14. 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

15. The following sets of policy options were considered.

Option 1: Scope of the guidelines:

16. Option A: providing guidelines on all aspects of internal governance arrangements including the assessment of the suitability of members of the management body, remuneration and disclosures.

17. Option B: providing guidelines only on the aspects that have not been dealt with in other EBA products.

18. Option A might appear to be more efficient for the addressees, as all the guidelines on this particular area would be accessible in a single document. The costs of implementing a single set of guidelines and separate sets of guidelines would be the same.

19. Option B would allow for greater differentiation between guidelines on internal governance arrangements, sound remuneration policies and suitability. Regarding the legal mandates provided to the EBA, Option B would reflect better the Directive 2013/36/EU mandates. In any case, all EBA guidelines can be accessed via the EBA Single Rulebook.

20. Option B was retained.

Option 2: Reinforcement of the involvement of the management body, particularly regarding risk oversight

21. Option A: no further guidelines, as the previous guidelines are sufficient.

22. Option B: reinforcement of the involvement of the management body regarding risk oversight by strengthening its duties and responsibilities, and distinguishing between the management body in its supervisory function and in its management function. In particular, it should be established that the management body in its supervisory function should monitor that the strategic objectives, the organisational structure, and the risk strategy and policy, as well as other policies such as remuneration and disclosure obligations, are implemented consistently. The management body in its management function should implement 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.

23. Option A is not recommended, as it would not lead to greater harmonisation and would not improve risk management practices or result in the greater involvement of the management body in risk oversight or more generally in internal governance arrangements.

24. Option B would increase risk oversight by the management body and risk culture within institutions in line with international standards. While some additional guidelines would be provided regarding the responsibilities of the management body, it is not expected that this would increase the costs of the governance arrangements already implemented within institutions or of supervision by competent authorities. Assessing and increasing the qualifications and the available resources of members of the management body, particularly regarding risk management, would tigger some costs. The costs would depend on the size and complexity of the institution.

25. Option B was retained.

Option 3: Proportionality

26. The approach taken was not sufficiently effective and did not lead to an appropriate level of harmonisation, as only a reference to the principle was made in the previous guidelines. Options for the approach to proportionality were as follows.

27. Option A: retaining the neutral approach taken under the previous EBA guidelines.

28. Option B: providing a set of criteria, in line with Article 74(2) of Directive 2013/36/EU, for the application of proportionality principle in a harmonised way.

29. Option A would not be in line with the EBA's mandate to develop guidelines to ensure the harmonisation of supervisory practices on internal governance arrangements, taking into account the proportionality principle.

30. Option B provides a non-exhaustive list of criteria to be taken into account in applying the principle of proportionality. All institutions and competent authorities should take into account at least those criteria, which will ensure consistency in the application of the proportionality principle. No additional costs would be created by these additional guidelines for both competent authorities and institutions.

31. Option B was retained

Option 4: Organisation of internal control functions, particularly the risk management function

32. Option A: no further guidelines, as the previous guidelines are sufficient.

33. Option B: strengthening the guidelines with regard to the resources, authority and stature of the risk management function only.

34. Option C: strengthening the guidelines with regard to the resources, authority and stature of all internal control functions.

35. Option A is not recommended, as it would not lead to greater harmonisation and would not improve risk management practices or result in the greater involvement of the management body in risk oversight or more generally in internal governance arrangements.

36. Option B is not recommended, as it may create inconsistencies regarding the organisation, resources and stature of the internal control functions within institutions, even though the principle of proportionality needs to be taken into account when implementing the guidelines.

37. Option C would create consistency between the internal control functions. While one might argue that this would cause additional costs, those costs are needed to establish a sound internal control framework and ensure the independence of the internal control functions. This is already required by existing regulations. However, stronger internal functions within institutions might be more costly in terms of staff costs or reorganisation; on the other hand, institutions would also benefit from the improved framework, which would lead to a better alignment of risk profile with risk appetite as set by the management body.

38. Option C was retained.

E. Cost-benefit analysis

39. Respondents to the public consultation found it difficult to assess the costs of the implementation work needed under the updated guidelines. The burden would be greater if all the guidelines needed to be applied on an individual level by all subsidiaries. A few respondents stressed that the development of ethical standards for external service providers would create additional costs. The guidelines might lead to a need for more staff for governance arrangements. Respondents pointed out the effect on the level playing field in relation to third countries.

40. While the guidelines are applicable to all institutions, regarding other subsidiaries they apply only on a consolidated or sub-consolidated basis and not on an individual level. Directive 2013/36/EU is to be applied to all subsidiaries on a consolidated basis and therefore related burdens are not incurred by implementing the guidelines. Sound ethical standards are key to protecting an institution's reputation. This holds true also where services are provided by external sources. The guidelines were adjusted and require institutions to take into account the ethical standards in place at service providers when selecting them. Overall, the initial assessment has not changed; in particular, the requirements regarding the independence of members of the management body and the composition of committees have been made lighter after taking into account the responses to the public consultation.

41. Overall, the guidelines, compared with the baseline scenario, will create very low additional recurring costs for institutions, mainly driven by reorganising their internal control frameworks. In addition, the minor increase in costs will be compensated for by the adoption of a more proportionate approach with clear criteria and by the additional benefits in terms of effective and sound internal governance arrangements. The implementation of the guidelines will improve internal governance within institutions and therefore reduce their vulnerability. Sound internal governance and conduct of business helps to build up trust in the banking system.

42. The implementation of the guidelines by competent authorities will trigger low one-off costs to change existing rules/methodologies/manuals and to inform staff members and the sector regarding those changes. As the changes are limited and will mainly involve updating existing guidelines, the costs should be relatively low.

43. Furthermore, the guidelines are in line with international internal governance standards; therefore, no impact on the level playing field in relation to non-EU institutions is expected.

5.2. Feedback on the public consultation

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

The consultation period lasted for three months and ended on 28 January 2017. Thirty-three responses were received, of which twenty-eight were published on the EBA website.

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

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

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

Summary of key issues and the EBA's responses

A key issue raised by many respondents is the applicability of the guidelines to different governance structures. Respondents were of the view that some provisions of the guidelines are not enforceable in or are not compatible with some governance structures adopted in Member States. For instance, in one-tier structures institutions have a unitary and inseparable body through which both management and supervisory functions are performed and where all members have the same responsibilities. Under some company laws, the body appointed by shareholders does not have executive functions and therefore some respondents felt that no requirements should be addressed to the management body in its management function; rather, they should be addressed to the senior management. A few respondents identified particular aspects that they deemed inappropriate for two-tier structures and for particular business models and/or governance systems, such as public or cooperative institutions. Overall, respondents advocated ensuring that the EBA guidelines are compatible with all governance models. In this context, some respondents believed that the definitions of the management body in its different functions should be clarified and that the notion of senior management should be used in the guidelines; in particular, 'senior management' should be included in the 'management body in its management function'. In addition, it was argued that the notion of key function holders should not be part of the guidelines, as it is not included in Directive 2013/36/EU.

Regarding the establishment of committees, many respondents deemed the guidelines to be too detailed, endangering the desirable flexibility granted under national laws. A few respondents pointed out that there could be unintended consequences, such as the building of inefficient and too large boards.

Another key issue identified concerns the scope and the level of application of the guidelines. First, respondents asked for confirmation that the guidelines do not apply to subsidiaries that are themselves not subject to Directive 2013/36/EU on a solo basis, but only on a consolidated basis. The situation of investment firms to which Directive 2004/39/EC, but not Directive 2013/36/EU applies should also be clarified. Second, some respondents asked for the group context to be better taken into account and suggested, in line with the principle of proportionality, applying lighter requirements to subsidiaries or allowing exclusions, arguing that subsidiaries should be allowed to rely on the group with regard to several matters (e.g. reporting, the code of conduct, the description of the operational structure, the internal control framework). It was argued that, with the same objective of decreasing the administrative and compliance burden, it should be made clear that proportionality applies to all the requirements of the guidelines.

Respondents found that parts of the guidelines (the references to the audit committee, the requirements on the composition of committees and the requirement to have independent members on the risk and nomination committees, the guidelines on reporting breaches to competent authorities, etc.) lacked a solid legal basis, because they went beyond what Directive 2013/36/EU explicitly requires. Respondents also suggested that the definition of 'independence' should be left to national law.

Respondents recommended that the three lines of defence model should be better defined and explained, while ensuring that the responsibilities of the first line are clearly set out.

The EBA has analysed and considered all the responses to the public consultation. The guidelines have been revised so that they can be applied to all possible governance structures. It is neither the intention to require institutions to change their governance structure, nor to alter the assignment of responsibilities as set out in national law. The guidelines clarify the meaning of 'management body' provided in Directive 2013/36/EU. They also clarify that any reference to the management body should be understood as including not only the members of the body appointed under national law but also the persons directing the business (e.g. the CEO or executive committee). The guidelines do not use the term 'senior management', as the definition is not precise enough and has been implemented by Member States in different ways. Using the concept of senior management in the guidelines would not lead to the appropriate level of harmonisation. The requirements on board committees have been revised to better reflect the principle of proportionality and other international standards.

Article 109 of Directive 2013/36/EU determines how the governance requirements should be applied. Institutions that are subject to that Directive have to apply the requirements on an individual basis. Regarding subsidiaries that are not subject to Directive 2013/36/EU, including MiFID firms not subject to Directive 2013/36/EU, the requirements are applied in a group context on a consolidated or sub-consolidated basis. The principle of proportionality should ensure the appropriate application of the requirements on all levels. Institutions are expected to adopt and implement group policies and, naturally, with regard to the performance of tasks, governance arrangements existing within the group can be relied on, while the management body of an institution has overall responsibility for that institution and its governance arrangements.

In accordance with Article 16 of the EBA Regulation, the EBA has the power to issue guidelines in the area of its competence. The area of governance, including the supervision of institutions' governance arrangements, is clearly included in this area (e.g. Article 74 of Directive 2013/36/EU). It is not necessary for certain concepts to be explicitly mentioned in the Directive in relation to the issuing of guidelines by the EBA. The EBA is not restricted to issuing guidelines based on an explicit mandate from the co-legislators. The concepts of key function holders, codes of conduct, independent directors, etc., are clearly linked to institutions' governance arrangements and therefore the EBA has the power to issue guidelines on these topics.

The guidelines are compatible with the three lines of defence model and it has been clarified that the business units (the first line of defence) are part of this model. However, the guidelines focus in particular on the responsibilities of the management body and the second line of defence. It was not deemed necessary to refer explicitly in the guidelines to the three lines of defence model; as the purpose of the guidelines is to specify regulatory requirements that are linked to certain functions, such explanatory text was not required. The structure of the guidelines has been changed to better differentiate between the internal control framework, in which all three lines of defence participate, and the specific requirements in relation to the second line of defence.

The principle of proportionality, a principle that applies to all EU legislation, applies to the guidelines. This means that the guidelines are to be applied taking into account the size of the institution and the nature, scale and complexity of its activities.

The feedback table contains a more detailed analysis of the comments made.

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

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
General comments			
Neutral approach on governance systems	Even though the draft guidelines do not advocate any particular structure and are intended to apply to all existing governance structures, they appear to be unsuccessful in the aim of creating guidance that can easily be applied to all sorts of governance structures. For this purpose, the following suggestions are proposed: • expressly state that the guidelines do not intend to give guidance on the allocation of tasks between different legal and organisational bodies; • adopt a more neutral wording that does not implicitly reveal that a certain governance model is assumed; • expressly clarify that, when the term 'management body' is used, it refers to either the management function or the supervisory function and that the tasks allocated by the management body are to be allocated to the correct body under applicable national law.	The comments have been accommodated. The guidelines do not advocate any particular governance structure and are not intended to change the responsibilities assigned by national law.	The guidelines have been amended to better apply to all governance systems.
Prescriptiveness	The wording of the guidelines is often prescriptive, as if the draft guidelines were a regulation. This prescriptive/regulating approach of the draft guidelines towards institutions' corporate governance practices is not compatible with the legal status of guidelines.	In line with the EBA's mandate, the approach of the guidelines is to specify the requirements of Directive 2013/36/EU and set out which arrangements are expected within robust governance arrangements. The guidelines respect all different company laws and the principle of proportionality and leave sufficient room for implementation by	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	The draft guidelines should focus exclusively on the harmonisation of supervisory practices and not on the harmonisation of corporate governance practices; the latter should be only a by-product of the former and not the other way round. One respondent suggested that a reference to national implementing laws should be included.	institutions. The guidelines set out several governance principles, which aim to establish appropriate checks and balances. With regard to competent authorities, guidelines are subject to a comply or explain approach, i.e. if part of the guidelines would contradict national law the competent authority has the option to not comply with the relevant part of the guidelines. Institutions should make every effort to comply with the guidelines. Institutions must comply with applicable law. Preserving in all cases existing national law would limit future harmonisation.	
Risk management	The guidelines should refer to 'risk control' instead of 'risk management', as the latter term includes some functions and activities that are allocated to the first line of defence.	Article 76 of Directive 2013/36/EU refers to the independent risk management function. The guidelines are consistent with the terminology used in the Directive. The change of terminology from the previous guidelines is explained in the background section.	Background section amended.
Reporting of breaches to competent authorities Section 10	The guidelines relate to the internal governance of institutions; therefore, the reference to the reporting of breaches to competent authorities is an element out of their scope that should be eliminated.	The EBA is mandated to provide guidance in the area of its competence. Article 71 of Directive 2013/36/EU sets out requirements for the reporting of breaches. A specific mandate set out in Directive 2013/36/EU is not necessary for every element of the guidelines. Establishing whistleblower channels is a measure to facilitate the supervision of banks and is therefore within the scope of the EBA's competences and is part of the task of supervising institutions' internal governance.	No change.
Mandate to provide guidelines, rationale and objective of the guidelines	A few respondents question if the EBA is mandated to provide guidance on, for example, the independence of members of the management body, committee structures, the audit committee or other aspects on which guidance was not explicitly required by Directive 2013/36/EU.	The EBA is mandated to provide guidance in the area of its competence. The requirements of Directive 2013/36/EU in the area of governance include only a few specific technical criteria that the EBA is to take into account when providing guidelines on Article 74(1) and (2) of this Directive. Article 74(1) sets out principles to be further specified by the EBA; this further	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		specification includes the guidelines in the areas mentioned, which fall under the mandate, as they concern institutions' robust governance arrangements and internal organisation. In accordance with Article 16 of Regulation (EU) No 1093/2010, the EBA can issue guidelines addressed to competent authorities or financial institutions with a view to establishing consistent, efficient and effective supervisory practices within the European System of Financial Supervision, and to ensuring the common, uniform and consistent application of Union law,	
Responses to questions in Consultation Paper EBA/CP/2016/16			
Background, paragraph 20; Section 12 Three lines of defence model	The three lines of defence model should be better explained and more guidance given on how it should be applied. The text on the risk management function should emphasise the importance of senior management and business line managers in identifying and assessing risks critically rather than relying only on surveillance conducted by the risk management function. Par. In addition, ensuring compliance is primarily a task for the first line. The word 'ensure', when tasks to be performed by the second line are referred to, should be reviewed, as this 'ensuring' is mainly a responsibility of the first line, while the second line adds an additional layer of control.	The text in the background section regarding the three lines of defence model has been further clarified. The word 'ensure' stresses that the objective of the measures taken by the second line of defence is to make certain of, for example, the compliance of the institution with internal and external requirements.	Par. The guidelines have been amended in several places to better explain the three lines of defence model.
Subject, matter, scope			

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
and definitions			
Date of application	Some respondents ask for sufficient time to implement the guidelines, at least one year.	The guidelines add only a limited number of requirements to the existing governance guidelines. However, to allow for legal changes that might be needed and to align the timeline with that of the EBA guidelines on the assessment of the suitability of members of the management body and key function holders, the guidelines will enter into force on 30 June 2018.	No change.
Scope	Several respondents suggest clarifying the application of the guidelines in groups. For this purpose, the following main suggestions are submitted: • the application on a consolidated basis cannot result in the same level of constraint than the application on an individual basis; • more proportionality should be adopted, allowing subsidiaries to benefit from exemptions or at least lighter requirements; • fully owned subsidiaries should not have all the same requirements to fulfil as heads of groups or listed entities; • a general principle should be added to allow the possibility of relying on existing processes or rules defined at group level; • only entities subject to Directive 2013/36/EU (CRD IV) should apply CRD IV rules on an individual basis. Entities not subject to CRD IV but which are parts of the consolidated perimeter of an entity subject to CRD IV should apply CRD IV rules only on a consolidated basis; • some respondents suggest specifying that key	Article 109 of Directive 2013/36/EU requires that the governance requirements are applied on an individual basis, unless competent authorities make use of the derogation provided for in Article 7 of Regulation (EU) No 575/2013 or Article 21 of Directive 26/2013/EU. In addition, it requires that the requirements are applied on a consolidated or sub-consolidated level to all subsidiaries. With regard to subsidiaries in the scope of prudential consolidation that are not subject to the Directive, the parent undertaking must be required by the competent authority to meet the obligations of Title 7, Chapter 2, Section II of Directive 2013/36/EU on a consolidated or sub-consolidated basis. Exceptions are possible only in line with the Directive and Regulation. Neither the guidelines nor the principle of proportionality can lead to the non-application of or exemptions from explicit regulatory requirements. Institutions within the scope of consolidation may as far as possible rely on or make use of the structures, processes and documentation established and may adopt group policies or base their policies on such group policies, e.g. where changes are needed to comply with national law. The scope section explicitly refers to and is consistent with	Sections 8 and 9 amended and other sections clarified.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	function holders should be considered only at the level of the parent company; • some respondents also stress that clarification of the application of the guidelines in groups would avoid the duplication of documentation and formalities within the group itself.	Article 109 of Directive 2013/36/EU.	
Question 1 General comment	With regard to cases where the 'management body' is mentioned without specifying whether in its management or supervisory function, some respondents suggest clarifying that this means the management body in its management function; others suggest that the guidelines should expressly provide that national corporate law will determine if the requirement will apply to the management body in its management or in its supervisory function. Some respondents suggest more clearly defining, including in the definitions section, the notion of 'management body'. With regard to its composition, it should be clarified that the management body must include not only the board of directors but also the CEO, the members of the executive committees, and the general manager or other senior managers, who will take responsibility for the executive management of the bank even if they are not part of the board.	The responsibilities of the management body, including in its management (executive) and supervisory (non-executive) functions, differ depending on the governance structure and national company law. Further specification in the guidelines is often not possible, as the guidelines do not intend to interfere with the responsibilities assigned under national company law. The responsibility is to be assigned to the responsible function within the management body under national law. In some cases, responsibilities may even be with the shareholders or owners directly. The definition of 'management body' in Article 3(7) of Directive 2013/36/EU indeed includes not only the body or bodies appointed in accordance with national law but also the persons who effectively direct the business of the institution. The management body is therefore sometimes broader than the governance body or bodies under national law, and always includes the persons who direct the business (e.g. the CEO, the executive committee or similar staff) in cases where they are not part of the governance body or bodies appointed by shareholders. The guidelines have been clarified accordingly.	Scope section amended.
Question 1	Some respondents recommend introducing the concept of senior management to the guidelines.	The guidelines intentionally do not refer to 'senior management', as the definition in Article 3(9) of the Directive is not sufficiently clear. The understanding of that concept differs between Member	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		States. The guidelines therefore introduce the concept of key function holders to achieve a greater level of harmonisation.	
Definitions Risk appetite	Some respondents observe that the current guidelines include two definitions: risk appetite and risk capacity. The definitions differ and are narrower than the definition in GL 44.	The definitions have been aligned with those used by the BCBS. The change of definitions has been explained in the background section.	Background section clarified.
Definitions Staff	Some respondents deem that this definition overextends the Level 1 scope. Respondents suggested deleting the reference to 'including subsidiaries not subject to Directive 2013/36/EU'. Some respondents suggest clarifying if contractors are included.	The definition of 'staff' covers the scope of application in accordance with Article 109 of Directive 2013/36/EU. It has been clarified that all subsidiaries within the scope of consolidation are included. Where institutions contract tasks through a service provider, the natural persons providing the service are not employees of the institution.	Definition clarified.
Definitions CEO	Some respondents suggest that this definition should emphasise responsibility for day-to-day management, since the reference to steering of the overall business could be misinterpreted as meaning 'being responsible for the institution's strategy'.	The CEO is a person directing the business. Referring to day-to-day management would lead to confusion with the concept of senior management defined within the Directive, which is implemented differently in Member States.	No change.
Definitions CFO	Some respondents deem that the CFO should not be included in the guidelines. Other respondents propose deleting the reference to 'and risks'.	The definition has been retained, in order to ensure that the CFO, if not part of the management body, is assessed as a key function holder. The reference to risk has been deleted.	Definition amended.
Definitions Head of internal control	Some respondents suggest replacing this definition with specific definitions of 'chief compliance officer (CCO)', 'chief risk officer (CRO)' and 'chief audit executive (CAE)', and clarifying that these functions are to be	The definition has been retained to be consistent with the guidelines on the assessment of the suitability of members of the management body and key function holders. The group application has been clarified (see above).	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	considered at group level only.		
Definitions Mandate regarding key function holders	Some respondents complain about the lack of a legal basis in Article 91 of CRD IV for the guidelines setting out requirements on key function holders and request their deletion.	Article 16 of the EBA Regulation lays down the general competence to issue guidelines with a view to establishing consistent, efficient and effective supervisory practices within the European System of Financial Supervision and ensuring the common, uniform and consistent application of Union law. However, the EBA may only issue guidelines within its scope of action, which is defined in Article 1(2) and (3) of the EBA Regulation. In accordance with Article 1(2), the limitation of power is clearly marked: the EBA must act only within the scope of the listed EU directives/regulations and of any further legally binding Union act that confers tasks on the EBA. Directive 2013/36/EU is one of the directives listed and internal governance is expressly covered in Article 74 of the CRD. Moreover, Article 74(3) of Directive 2013/36/EU expressly mandates the EBA to issue guidelines on the governance arrangements, processes and internal control mechanisms referred to in Article 74(1). In addition, corporate governance is expressly mentioned in Article 1(3) of the EBA Regulation among the matters on which the EBA is allowed to act in the field of the activities of credit institutions and investment firms. Ensuring the suitability of key function holders of credit institutions and their role in institutions is an essential part of the internal governance arrangements for the prudent management of an institution. Moreover, in accordance with Article 98(7) of the CRD IV, such governance arrangements must be expressly included in the review and evaluation to be conducted by competent authorities.	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Definitions Key function holders	Some respondents request the deletion of the reference to 'other key function holders'. Others ask for it to be clarified to whom this definition might apply.	Certain key functions are specifically named in the definition, while it is for the institution to determine who other key function holders are.	No change.
Definitions Significant institutions	Some respondents deem it inopportune that the guidelines provide a further definition of 'significant institutions' and propose replacing this with a reference to 'systemically important institutions'.	The definition of 'significant institutions' is used in several EBA guidelines and consistent with Directive 2013/36/EU. Competent authorities can also determine whether an institution is significant for their market.	No change.
Definitions Conflict of interest	Some respondents suggest better reconciling this definition with the fact that members of the management body always have to pursue the benefit of the entity first, but typically also have to consider the interests of all shareholders, employees and other stakeholders. Otherwise, it could lead to the unacceptable consequence that shareholder representatives on the supervisory board would have to abstain from their voting right when decisions regarding the annual accounts and the possible dividends had to be made. Some respondents suggest clarifying why the definition appears to exclude internal conflicts.	The definition has been deleted and additional guidance has been provided. Institutions should have a specific conflict of interest policy for staff. Staff includes the members of the management body of the institution. The conflict of interest policy for staff deals with conflicts between the personal interests of staff and the interest of the institution. Institutions should also manage other conflicts of interest, e.g. between different group entities, business lines or units, or between the institution and external stakeholders, including clients. The purpose and application of a conflict of interest policy has been clarified.	Definition deleted and Section 10.3 amended.
Proposed additional definitions	Some respondents recommend adding additional definitions for: 'competent authorities', 'chief risk officer (CRO)', 'conduct risk' (in line with EBA/GL/2014/13), 'compliance risk' (in line with GL 44) and the 'three lines of defence' (in line with BCBS principles).	Definitions of 'compliance risk' and 'conduct risk', which are a subset of operational risks, are not needed in the guidelines. The chief risk officer in the guidelines is the head of the independent risk management function. As neither the term 'CRO' nor the term 'three lines of defence' is used in the guidelines, definitions are not needed. The three lines	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		of defence model is explained in the background section.	
Paragraph 17	Some respondents observe that this provision is in conflict with national law in countries where different governance structures are applied (e.g. there is only one management body responsible for functions that the guidelines distribute between the management function and the supervision function). Other respondents ask that the responsibilities of the management body, distributed between the 'supervisory function' and the 'management function', be better expressed, ensuring that the supervision tasks include the task of strategic direction and the approval of main transactions, as well as the task of monitoring and controlling the management body performing its management function.	The paragraph has been amended so that it can be applied to all different governance structures. Further specification of the responsibilities of the different functions beyond what is already included in the guidelines is not necessary and could conflict with national company law.	Guidelines amended.
Paragraph 19 Responsibilities of the management body	Some respondents suggest also mentioning the board's responsibility for setting the general principles for the development of human resources (i.e. talent management, succession planning, etc.).	See comment on paragraph 17.	No change.
Question 2 Paragraph 19(h)	Some respondents deem not only that this requirement is hard to reconcile with the purpose of the law but also that the inclusion of the minutes of the discussion could ultimately prevent or hamper discussion between the members of the management body. Therefore, it is suggested that the guidelines simply require the decision taken to be documented without specifying any further obligation.	The committees give advice and recommendations to the supervisory function and support it. The comment has been accommodated and the text has been clarified.	Paragraph 19(h) amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Paragraph 19(j)	Some respondents suggest exempting very small and non-complex institutions from adopting a code of conduct. Some respondents suggest clarifying that institutions may rely on a group-wide or sector-wide code of conduct.	All institutions should have a code of conduct or similar. Setting an appropriate culture is a core principle of robust governance arrangements. Institutions may adopt and implement group policies or common policies, e.g. provided by associations.	Section 10.2 clarified.
Paragraph 20	Some respondents suggest that the term 'communications' be explained and narrowed in scope, assuming that it means external communications (particularly investor relations, business reporting).	The comment has been accommodated.	Paragraph 20 amended.
Paragraph 23 Supervisory function of the management board	Some respondents observe that supervision seems to be entrusted to non-executive members only, with no chance for the executive members of the management body to take part in it. Responsibility for strategic supervision is with the board as a whole and not with individual non-executive members. Some other respondents suggest that the management body in its supervisory function should not be understood in all cases as a mere monitoring and overseeing body. The focus on board monitoring should be balanced by a correspondent emphasis on the strategic function of the board, consisting in developing the organisation and its strategy. It is suggested that the guidelines be more balanced on this topic. Some respondents suggest amending the reference to the fact that 'the management body in its supervisory function should also ensure the integrity of the financial information and reporting, and internal control	The guidelines have been altered so that they can be applied to all governance bodies. The supervisory function may, where the national company law allows, include executive and non-executive members. Its main focus is oversight tasks. The oversight role of the supervisory function includes overseeing the management function, the achievements of objectives, challenging the institution's strategy, monitoring and scrutinising the integrity of financial information and reporting, and the internal control framework, including effective and sound risk management.	Paragraph 23 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	framework, including effective and sound risk management' in order to make it applicable also to institutions belonging to Member States where national corporate law does not confer such tasks on the management body in its supervisory function. Therefore, the following amendment is proposed: 'the management body in its supervisory function should ~~also~~ **submit recommendations or proposals to** ensure the integrity of financial information and reporting, and the internal control framework, including effective and sound risk management'.		
Question 3 Paragraph 24(a)	Some respondents suggest the following drafting amendment: 'a) have suitable members who do not perform any executive function in the institution and are **collectively** able to fully understand and oversee the risk strategy and the risk appetite of the institution;'. Other respondents suggest that the board should have 'a majority of suitable members who do not perform any executive function in the institution'.	The issue is dealt with in the EBA guidelines on the assessment of the suitability of members of the management body and key function holders. All members of the management body individually and the management body collectively must be suitable. While in most cases institutions have more non-executive directors than executive directors, it was not seen as necessary to issue guidelines on this fact.	Subparagraph deleted.
Paragraph 24(e)	In some jurisdictions, the management body in its supervisory function may have to not only 'oversee and monitor the strategic objectives' but also decide on the strategy.	The guidelines focus on the oversight role of the supervisory function, which under national law may have additional responsibilities. This has been clarified.	Paragraph 24 amended.
Paragraph 24(g)	Some respondents suggest amending this paragraph in order to make it applicable also to institutions adopting a governance structure under which the relevant national corporate law does not allow or permit direct reporting of the internal control functions to the	In line with Article 76 of Directive 2013/36/EU, it must be possible for the risk management function to report directly to the supervisory function. All control functions should be able todirectly access to the management body in its supervisory function, so that, where	Paragraph 24(g) amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	management body in its supervisory function.	necessary, they can warn that function about adverse developments. The wording has been clarified.	
Paragraph 24(i)	Some respondents deem that this should be the responsibility of the audit committee rather than of the whole board, while the board should receive a regular report from the internal audit function through the audit committee on significant audit findings.	While the main tasks will be performed by the audit committee, where established, the final responsibility for the audit plan is with the management body.	No change.
Paragraph 29	Some respondents suggest amending this paragraph in order to make it applicable also to two-tier systems.	The comment has been accommodated.	Paragraph 29 amended.
Section 3 Role of the chair of the management body	Some respondents comment that the chair of the management body should be both independent and a non-executive member. Some respondents suggest clarifying if the guidance on the chair is applicable to the management body in its management or supervisory function (or both). Some respondents suggest that the guidelines should put greater emphasis on the relevance of the personal attitudes of the chair.	The EBA guidelines require, in line with the BCBS principles, that the chair is independent or a non-executive-member. In addition, Directive 2013/36/EU and the guidelines allow, in exceptional cases with the approval of the competent authority, that the chair can be the same person as the CEO. The chair is, in line with Article 88 of the Directive, the chair of the supervisory function. In a unitary board system, the differentiation suggested is not possible. When reading the guidelines, applicable company law has to be taken into account. The assessment of the chair's skills is part of the assessment of his or her suitability, which needs to take into account the position of a member of the management body.	No change.
Question 3 General comments	Some respondents highlight that the guidelines do not duly take into account the circumstance that some national corporate laws provide specific rules on the composition of certain corporate bodies (e.g. the management board in its supervisory function of public/cooperative banks is elected by the local	Institutions, including institutions where a member of the management body represents the Member State, have to comply with all legislative requirements. While there may be limitations on the possibility of influencing the composition of the management body, its proper functioning must still be ensured. The requirement that at least two persons must effectively direct	Section on the management body revised.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	parliament). This limits the possibility of influencing the composition of the management body. Some respondents suggest clarifying that, in compliance with national corporate laws, collegiality in the management function can also be limited to two people (CEO, deputy CEO). Some respondents point out that the responsibilities of the management body sometimes seem to include tasks that are too operational.	the business is already clearly encoded in Article 13 of Directive 2013/36/EU. Therefore, no further clarification is needed. The management body, while being responsible, for example, for the implementation of the institution's strategies, may of course rely on other staff for the tasks necessary to, for instance, implement policies.	
Section 5 Specialised committees of the management body in its supervisory function	Some respondents observe that the requirement to create different specialised committees composed of independent members and having independent members as chairs would lead to very large boards, which might reduce the efficiency of the management body. Some respondents deem that the requirements on the different committees are too detailed and ask for a more flexible approach. Some respondents observe that some national corporate laws do not allow the issues to be dealt with by the specialised committees (compliance, risk management, internal control, reporting) to be delegated by the board; consequently, such issues remain competences of the board. Some respondents suggest that Section 5.2 should not apply to non-significant institutions.	Significant institutions are required to form risk, nomination and remuneration committees. Other institutions may also form such committees but are not obliged to do so. The principle of proportionality applies. The section has been revised to distinguish between the situation of G-SIIs, O-SIIs, other significant institutions, designated by competent authorities or national law and the situation of other institutions. In addition, the independence criteria have been reviewed and it has been clarified that meeting a criterion results in a refutable presumption that the member is not independent. Committees act under the overall responsibility of the management body.	Section 5 revised.
Paragraph 32	Some respondents suggest further clarifying how specifically it can be ensured that the board's decision-	It is for the institution to ensure that the composition of the	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	making process is not dominated by a member or a small set of members.	management body is appropriate.	
Paragraph 33	Some respondents suggest redrafting the guidance on information flow to the supervisory function in order to specify that generally information should be provided in the normal course of business without undue delay. Only information regarding material developments should be provided without delay.	The comment has been accommodated.	Paragraph 33 amended.
Paragraph 34	Some respondents highlight that this paragraph seems only to allow committees to provide advice to the management body without granting them any authority to assume decisions. Therefore, they suggest that 'and to prepare the decisions to be taken by this body' be deleted.	The guidelines have been clarified. Decision-making powers may be delegated to committees if allowed under national law.	Paragraph 34 amended.
Paragraph 37	Some respondents do not fully agree on requiring that committees should not be composed mostly of the same group of members; the main reasons are that: - It is not practical, especially for smaller institutions and group entities. - Remuneration and nomination committees in particular often deal with overlapping issues. The same goes for audit and risk committees. - Sufficient flow of information and the proper performance of supervisory body functions can be ensured only if composition of committees by the same group of members is allowed.	Some cross-participation of members is allowed and ensures a sufficient information flow. The guidelines have been revised to allow a more practical approach to the composition of committees. See also comments on Section 5.	Section 5.2 amended.
Paragraph 42 Non-executives members of the	Some respondents suggest deleting any requirement for committees to be made up exclusively of non-executive directors.	In line with Directive 2013/36/EU and other international standards, the nomination and risk committees should be composed of non-executive directors. Committees may invite other staff, where needed, to their meetings.	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
committees			
Paragraph 42 Independent members on the specialised committees	Some respondents observe that CRD IV requires only that committee members are non-executives; no independence requirements are set. Therefore, they deem that the guidelines do not have a legal basis. Regarding the notion of independence: - Some respondents suggest deleting it or, otherwise, suggest that it should refer only to independence of mind. If it goes beyond independence of mind, it will cause problems for cooperative banks, for instance, since the applicable national law stipulates that every supervisory board member usually has to be a member of the cooperative as well. - Some respondents propose introducing a specific notion of independence applicable to fully owned subsidiaries in order to have no separation of liability and control. - Some respondents suggest that the independence criteria be left to national law or soft law and deleted from the guidelines. Regarding the number of independent shareholders in the specialised committees: - Some respondents require the guidelines to further explain why independent members should be the majority of the risk committee but should be just a	The EBA has the legal power to issue guidelines in the area of its competence, including on institutions' governance arrangements. Independence of mind is required of all members of the management body. 'Being independent' goes beyond this requirement. See also the feedback on the EBA guidelines on the assessment of the suitability of members of the management body and key function holders regarding 'independent directors'. Having at least some independent members of the management body in its supervisory function is required for all significant institutions and listed institutions, including subsidiaries, ensuring that the interests of all stakeholders are taken into account. Other institutions should have at least one idependent director, unless they are fully owned subsidiaries within a group.The necessary harmonisation of criteria to assess the independence of a member is not possible in the absence of requirements at the European Union level. See comments on Section 5.	Section amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	sufficient number in the other specialised committees. - Some respondents suggest clarifying that an appropriate number of independent members is required only if the institution is required to establish committees. - Some respondents ask for the meaning of 'sufficient' to be clarified. In order to ensure more flexibility, some respondents suggest adding the following: 'Where the member is not considered independent, the institutions can prove the independence of a member and/or decide on measures to mitigate possible conflicts of interest so that the member is independent afterwards. For example, the member should abstain from voting on any matter where a conflict of interest exists. This process and decisions should be documented.'		
Paragraph 43	Some of the respondents do not agree on requiring appropriate 'professional' experience of the members of the risk and nomination committees, deeming that the adjective 'professional' suggests that all members must be able to look back on a career as a risk manager. This requirement does not match those of Article 76(3) of CRD IV. That provision does not require any experience at all, but only knowledge, skills and expertise. Some respondents observe that requiring members of the committees to have such knowledge, skills and experience both individually and collectively would be particularly challenging in a two-tier system, where a very different set of individuals performs the	The comments have been accommodated. However, committees need to be composed in such a way that they have the collective knowledge and skills to perform their tasks.	Paragraph 43 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	supervisory function.		
Paragraph 44	Some respondents do not agree with requiring each chair of a committee to be independent, for the following main reasons: - Some deem that this requirement goes far beyond BCBS principles on corporate governance. The principle of proportionality has to be applied, as the BCBS principles are generally applied to G-SIIs. - Some highlight the impact that this requirement would have on group structures: it would mean that, for example, the CFO of an industrial enterprise that is the parent company of a credit institution would no longer be able to chair the risk committee or audit committee, which would weaken the position of the shareholder. - some deem it sufficient to provide that the chair must be a non-executive member. Some respondents deem that, especially for the nomination committee, it should be sufficient that the chair be a non-executive director. Having an independent, non-executive chair could be considered appropriate for the audit committee. Some respondents are of the view that the prohibition on a dual chair applicable to all the committees, and the proposed rotation requirement, would aggravate the problem of complying with all the existing requirements for the constitution of specialised committees.	The guidelines have been revised to better take into account the principle of proportionality and to differentiate between G-SIIs, O-SIIs, other significant institutions and other institutions. Independent members of the management body in its management function should always have an active role in committees. In G-SIIs and O-SIIs, the nomination committee should include a majority of members who are independent and should be chaired by an independent member. In other isignificant nstitutions, the nomination committee should include a sufficient number of members who are independent; having a chair of the nomination committee who is independent is considered a good practice in all significant institutions that have set up such a committee. In G-SIIs and O-SIIs, the risk committee should include a majority of members who are independent. In other significant institutions, the risk committee should include a sufficient number of members who are independent. In G-SIIs and O-SIIs, the chair of the risk committee should be an independent, non-executive member. In other significant institutions, the risk committee should be chaired, where possible, by an independent, non-executive member. In all institutions the chair of the risk committee should be neither the chair of the management body nor the chair of any other committee. The management body and its committees need to take into account the interests of all stakeholders and not only of the shareholders.	Section 5.2. revised.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Paragraph 45 Audit committee	Under Directive 2014/56/EU amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, the audit committee can be exempted from the independence requirements if all members of the audit committee are members of the supervisory body.	The comment has been accommodated. The guidelines refer to the audit directive.	Paragraph 45 amended.
Section 5.3 Committees' processes Paragraph 46	Some respondents deem that this paragraph may not be applicable to subsidiaries fully integrated in a group and suggest that it should be specified that, in such entities, the committees can rely on the existing processes of their parent company.	The guidelines do not prevent committees from implementing the processes defined by a parent institution.	No change.
Paragraph 46(a)-(b)	The requirement on access to information by the audit function should be clarified to make clear that it does not mean that the audit function should have direct access to IT systems, which might contradict data protection requirements. More guidance is needed on which data are relevant (paragraph 46(a)).	The requirement for access to relevant information and data does not mean that it is necessary to give committees unlimited access to all IT systems at all times. However, committees need to be able to acquire all the information that is necessary to perform their duties.	Paragraph 46 amended.
Paragraph 46(d)	Some respondents observe that this paragraph cannot be applied in certain governance structures.	Committees, where necessary, should involve other relevant functions. This per se is not limited by the governance structure adopted. The wording has been clarified.	Paragraph 46 amended.
Section 5.4 Role of the risk committee	Some respondents suggest that the specific tasks of the committee may differ depending on national company law. Some observe that certain roles of the risk committee are not applicable to a two-tier structure, where the supervisory board does not set the risk appetite, strategy or corporate culture (see subparagraphs (a) and	The risk committee should at least be responsible for the tasks set out in the guidelines. National law may assign additional duties. The language has been clarified and adjusted to suit all governance systems.	Section 5.4. amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	(d)).		
Paragraph 47(e)	Some respondents do not agree with this role, deeming that each corporate body should be entitled to appoint its own consultants. Others deem that the role of the risk committee should rather be limited to providing advice or support and that the committee should only receive regular information on the appointed external consultants.	The comments have been accommodated.	Paragraph 47(e) amended.
Paragraph 47(g)	Some respondents deem that this is an operational task of the management body that does not concern the supervisory body in two-tier governance structures. The risk committee's job should be overseeing but not executing. The word 'examine' should therefore be replaced by 'oversee'. Some respondents suggest that 'all' should be removed from 'financial products' and to limit the requirement to material products in order to make the requirement practical. A detailed review of all financial products by the risk committee would be too time-consuming. The risk committee should not have to examine the alignment between all financial products and services offered to clients and the business model and risk strategy of the institution, but should only receive, on an annual basis, a report on such alignment covering significant risks.	The wording of the guidelines has been adjusted to stress the oversight role of the risk committee. The oversight should focus on material financial products and services. The committee bases its assessments on reports received by the internal control functions directly or indirectly, but should form its own view on the risks that are associated with the products and services provided.	Paragraph 47(g) amended.
Section 5.5	Some respondents highlight that, pursuant to a	Where a different board is mandated with the tasks under	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Audit committee	governance model provided by their national legal framework (Italy), these tasks and responsibilities belong to a specific corporate body other than the management board, namely the board of statutory auditors. Therefore, this paragraph cannot be applied to institutions adopting this governance model.	company law, the guidelines on the audit committee should be interpreted as applying to that board.	
Paragraph 50(c)	Some respondents deem it more appropriate that the committee make recommendations to the board to ensure the adequacy of the financial reporting process.	The comment has been accommodated.	Paragraph 50 amended.
Paragraph 50(h)	A few respondents ask for clarification of the term 'review'.	The comment has been accommodated.	Paragraph 50 amended.
Paragraph 51 Combined committees	Some respondents ask why non-significant institutions need the permission of the competent authorities to combine risk and audit committees, if they are not required to form these committees.	A listed institution would be required to have an audit committee under the Audit Directive. Article 76(3) of Directive 2013/36/EU envisages that the approval of the competent authority is needed.	No change.
Section 6 Organisational framework and structure	Some respondents state that ensuring an appropriate organisational and operational structure is primarily the responsibility of the management. Some respondents observe that this section creates a heavy burden on institutions and suggest easing the requirements within paragraphs 56 and 57 by limiting the requirements to the material changes and the main organisational features. The adoption of a written organisational framework should be done at the level of the central body and not be required at the level of the regional or local cooperative banks affiliated to such a central body.	The substance of the requirements has not changed from the previous guidelines. The management body includes the persons who direct the institution. Paragraph 57 of the 'Know your structure' section has not changed from the previous guidelines. The application of policies in a group context has been clarified. Subsidiaries or affiliated institutions should adopt and implement group policies and make use of available documentation, but they need to meet the requirements on an individual level, unless a waiver is granted by the competent authority under Article 21 of Directive 2013/36/EU or Article 7 of Regulation (EU) No 575/2013/EU.	Paragraph 56 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Paragraph 60	Some respondents deem that this paragraph introduces excessively burdensome obligations on the management body of the consolidating institution. They observe that this approach might induce top executives to micromanagement, and ultimately result in a departure from the risk-based approach, a loss of focus on critical issues, and counterproductive effects.	There is no change from the previous guidelines other than the requirement that the institution needs to be able to provide information in a timely manner, which is not considered to be burdensome, as an institution's structure needs in any case to be documented. The provision ensures that the group's capital, liquidity and risks are managed in a holistic way. The requirement is fully consistent with Article 109 of Directive 2013/36/EU, which requires the application of governance requirements also on a consolidated basis.	No change.
Paragraph 61 Reporting obligations within groups	Some respondents deem that this is an obligation that is difficult to comply with. Under some national laws, restrictions might apply to the disclosure of information to third parties (including consolidated supervisory authorities). These cases should be duly mentioned in the guidelines. Additionally, the requirement to document any flow of significant information between entities and to make it available to competent authorities is deemed unnecessary.	The comment has been accommodated. Institutions should document information on their objectives, strategies and risk profiles on individual and consolidated levels and keep this information up to date. Although the reference to competent authorities has been deleted, it should be remembered that institutions are subject to supervision and that in this context competent authorities will request the necessary documentation from institutions.	Paragraph 61 amended.
Section 6.3 Complex structures and non-standard or non-transparent activities	Some respondents find that the guidelines are quite vague in this section, which may lead to differences in implementation and a non-level playing field in terms of protection against non-transparent activities. Some respondents, in order to clarify the obligations on institutions, suggest providing – in line with the OECD, the EU Common Reporting Standard and the EU Mutual Assistance Directive – that, where accounts are held by legal entities, the legal entity has to issue a so-called 'self-certification' stating whether it is an active or	The guidelines in this section set out clear principles. It is not possible to describe each and every case of potential complex structures or non-transparent activities. Institutions also have obligations to prevent, for example, money laundering or financing of terrorism conducted by clients. Hence the guidelines cannot be limited to the institutions' own structures but need also to cover structures set up by institutions for clients.	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	passive entity and, if it is a passive entity, to additionally indicate the persons controlling it. Some respondents observe that this section addresses both the issue of complexity in an institution's own organisational structure and the complexity issues related to client activities.		
Paragraph 67(b)	Fulfilling the obligation to report to the competent authority might not always be feasible due to data protection and/or tax secrecy issues.	The guidelines require reporting on the activities and risks of such structures. The protection of personal data is not affected by the provision.	No change.
Title II Internal governance policy, risk culture and business conduct			
Question 4 Section 7; paragraph 70 Reference to Annex I and requirement to have a written governance policy	Respondents consider that the management body in its supervisory function could be overloaded with tasks that are of an executive nature and not be able to efficiently ensure its supervisory mission. Some respondents point to the fact that there can be benefits to having one central document for the group, which avoids discrepancies and reduces the administrative burden. Referring to Annex I, some respondents comment that they are concerned that it is too broad; others comment that Annex I includes an exhaustive list of aspects to be considered in the internal government policy. However, there should not be a requirement to have a single document approved by the management body.	The guidelines have been clarified regarding the creation and adoption of group policies by subsidiaries. Institutions should document their governance arrangements and policies. Annex I lists all those arrangements and policies. It has been clarified that the documentation can be spread over different documents, but that a central document should be available that points to such existing documentation.	Section 7 deleted.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Question 4 Section 7, paragraph 72	Respondents consider that this paragraph is inconsistent in stating that it is the sole responsibility of the compliance function to 'analyse how the internal governance policy affects the institution's compliance with legislation, regulations and internal policies and should report all identified compliance risks and issues of non-compliance to the management body'.	The guidelines on the organisational framework and internal control framework have been clarified. Section 7 has been integrated into those provisions. Institutions are required to document their governance arrangements and policies. This can be done in separate documents and existing policies can be referred to. Ensuring compliance is not the sole responsibility of the second line of defence. The responsibilities of the control functions are set out in a specific section of the guidelines.	Guidelines clarified and restructured.
Paragraph 73	One respondent deems the periodic review of the governance policy by the supervisory board to be too prescriptive. This provision should therefore be deleted.	See comments on paragraph 72.	Guidelines clarified and restructured.
Question 4 Section 8; paragraph 75	(Mixed) financial holding companies should be included in the scope; according to Article 109 of CRD IV, parent undertakings and subsidiaries are obliged to fulfil governance requirements at group level. Some respondents point out that subsidiaries outside the scope of CRD IV seem to be wrongly covered by the scope.	The guidelines have been better aligned with the wording of Article 109 of Directive 2013/36/EU. The governance requirements apply also on a consolidated basis, which includes also firms that are not subject to the Directive on an individual basis. Holding companies are not directly subject to the requirements but need to ensure that the requirements of the Directive are complied with.	Paragraph 75 amended.
Question 4 Section 8	The use of the terms 'policy' and 'framework' should be aligned and the difference between the two explained.	The comment has been accommodated.	Section 8 amended.
Question 4 Paragraph 77	National legal requirements should obviously be taken into account at the national level but are clearly not manageable directly by the parent company and therefore should not systematically be taken into account in a group-wide policy.	The comment has been accommodated. However, in line with Article 109 of Directive 2013/36/EU, the parent undertaking and subsidiaries have an obligation to ensure that the subsidiaries comply with the governance requirements. Subsidiaries, when adopting group policies, should make the changes necessary to	Section 8 revised.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		comply with national law.	
Section 8; paragraphs 78 and 79	Paragraph 78 provides an application to subsidiaries established in third countries. This entails a competitive disadvantage compared with local entities, which may be subject to less restrictive local regulations.	The guidelines follow the requirements of Article 109 of Directive 2013/36/EU.	No change.
Section 8; paragraph 84(a)	It is not clear what 'outside the institution' means in this context. 'Staff should act in accordance with all applicable laws and regulations and promptly escalate observed noncompliance within or outside the institution.'	It has been clarified that there should be an information channel to the competent authority.	Paragraph 84 amended.
Section 8; paragraph 84(b)	The requirement for all staff to know and understand the risk capacity is deemed to be too far reaching.	The comment has been accommodated.	Paragraph 84 amended.
Section 9; paragraph 85	Respondents state that the implementation of ethical standards for external service providers lies beyond the power of the institutions. Some respondents suggest applying the principle of proportionality, thus exempting very small and non-complex institutions from adopting a code of conduct. Some respondents suggest clarifying that institutions may rely on a group-wide or sector-wide code of conduct.	Institutions may rely on group-wide policies or codes of conduct issued by other competent entities. The existence of a code of conduct should be taken into account in the procurement of service providers.	Paragraph 85 amended.
Section 9; paragraphs 85-87(c)	Several respondents ask for the wording of paragraph 87(c) to be changed because they think that defining a catalogue of acceptable and unacceptable behaviour is neither realistic nor necessary and argue that not all situations can be defined in advance.	The comments have been accommodated; examples of such behaviour are sufficient.	Paragraph 87(c) amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Section 9; paragraphs 88 and 89	Several respondents point out that it is not clear what the relationship between these two paragraphs is. One respondent suggests that it is sufficient to send reports on deviations to the management body and to send on an annual basis a report on how the implementation of and compliance with ethical and professional standards are ensured. The responsibility to review implementation and compliance should be allocated to the institution itself. One respondent suggests that such a review should be done by the compliance function.	The guidelines have been clarified. It is for the institution to define which function is in charge of monitoring compliance with the code of conduct. Periodic reporting has been retained; the guidelines allow for a sufficient level of flexibility for the appropriate reporting framework to be defined internally.	Paragraph 88 amended.
Section 9; paragraph 92	The provision contradicts the definition that conflicts of interest are conflicts between the private interest of a person and the interest of the institution. National laws may have specific requirements on conflict of interest policies.	The section has been clarified and deals now only with the conflict between private interests and the institution's interest. However, with regard to tasks within the institution that are incompatible or where conflicting interests of different business units exist, the institution has to implement appropriate arrangements (e.g. segregation of duties regarding conducting business and control). This has been clarified in the section on the internal control framework.	Section 9.3 revised.
Question 4 Paragraph 94(f)	One respondent is concerned about the requirement for binding consultative advice from independent members of the management body, as this is in conflict with national company law. Furthermore, requiring shareholder approval for most important transactions is in conflict with some company law; in addition, the role of statutory auditors has to be clarified in this context.	The guidelines provide examples of measures that can be used to manage conflicts of interest. Where the examples provided are in conflict with applicable law or where they are not practical, other measures have to be taken.	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Section 9; paragraph 95	Respondents suggest that the requirement to mitigate or remedy *any* conflict of interest should be limited to material conflicts of interest.	It is for the institutions to assess the materiality of conflicts of interest.	Section 9.3 revised.
Section 9; paragraph 97	Two respondents think that reporting breaches outside regular reporting lines should not prevent staff from reporting to their managers.	The comment has been accommodated.	Paragraph 97 amended.
Question 4 Paragraph 101	If the case should justify measures being taken against persons, such persons should still be protected against unjustified negative effects and should be protected by relevant confidentiality rules.	The comment has been accommodated.	Paragraph 101 amended.
Section 9; paragraph 103	The management body is a collegial body; making one member responsible is contrary to the principle of collegiality.	The comment has been accommodated. While the body is collegial, it is possible to assign certain tasks to one member.	Paragraph 103 amended.
Section 10; paragraph 104	Reporting of breaches to competent authorities should not be required, as it is not an element of internal governance.	The guidelines also deal with the supervision of institutions' governance arrangements.	Paragraph clarified.
Question 4 Section 10	If all employees are invited to report possible breaches of laws and regulations to the authorities, the authorities might end up receiving a large amount of information of varying value and quality. Reporting by individual employees could create unnecessary confusion and work both for the authorities and for the board.	See also Article 71 of Directive 2013/36/EU. Having in place not only internal but also external whistleblowing channels is an effective tool to improve institutions' governance and to detect material breaches of applicable laws. Reporting outside of the institution may in some cases lead to better protection of the whistleblower.	No change.
Section 11; paragraph 109	Some respondents suggest replacing 'e.g.' with 'i.e.', because the example in brackets is the only situation that could be considered outsourcing from a legal point	The comment has been accommodated.	Paragraph 109 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	of view.		
Title III Proportionality			
Question 5 Proportionality	Several respondents suggest that the provisions on proportionality should be moved to the beginning of the guidelines in order to clarify that they apply to the guidelines as a whole.	The title was moved and is now Title I. All EU legislation and guidelines are subject to the principle of proportionality; hence the change is only presentational.	Guidelines restructured.
Question 5 Paragraph 112	It should be clarified that the list of proportionality criteria is not binding and whether it is cumulative.	The assessment of proportionality always requires a case-by-case assessment of several aspects that are relevant for the specific institution. It has been clarified that additional criteria may be taken into account.	Paragraph 112 amended.
Title IV Internal control framework			
Question 6 General comment	Clarification regarding the relationship between the required recovery plans under the Bank Recovery and Resolution Directive and the contingency and recovery plans required by guidelines would have been very useful.	Business continuity management and bank recovery and resolution are unrelated topics. Business continuity aims to ensure the continuity of business in the case of disruption (e.g. following external events, natural catastrophes or IT failures).	No change.
Question 6 Section 12; paragraph 113	It is suggested that 'strong' be deleted in both the first and second sentences because it is an indeterminate legal concept. The delineation between the three lines of defence is not clear.	The comments have been accommodated.	Paragraph 113 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Paragraph 116	Some respondents point out that it should be possible to develop the governance framework within the group; the individual institutions would simply adhere to the group standard.	The application of standards within a group has been clarified.	Paragraph 116 amended.
Paragraph 119	It is not clear which function is responsible. This could be clarified by adding 'in their respective area of responsibility'.	The comment has been accommodated.	Paragraph 119 amended.
Question 6 Section 12; paragraph 122	One respondent points out that the guidelines allow the head of internal control functions to be subordinate to a senior executive who is not responsible for managing the activities monitored by the internal control area. CRD IV envisages that the head of risk will report directly to the management board in its supervisory function. For others, it is not compatible with national corporate laws in accordance with which the supervisory body is responsibly 'only' for overseeing the management body and not for overseeing the levels below the management body. It should be clarified that the heads of internal control functions have to report directly to the CEO, although they should have direct access to the board of directors.	The guidelines have been amended so that they can be applied to all governance structures. It is obvious that the control functions have regular reporting lines to the management body in its management function. The heads of control functions should have direct access to the supervisory function and report to it when necessary, e.g. to warn it about adverse developments. In order to ensure that the control functions are independent, they cannot be subordinate to senior executives who are also responsible for managing business areas that are controlled by those functions.	Paragraph 122 amended.
Paragraph 123	Direct reporting lines from the heads of the internal audit and risk management functions to the supervisory board are not in line with national company laws.	According to Article 76 of Directive 2013/36/EU, the risk management function must be able, where necessary, to have direct access to the supervisory function. The same should apply to the compliance and audit functions so as to ensure, where necessary, their independent reporting on issues to the supervisory function or the audit committee, e.g. regarding issues	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		that pose material risks.	
Section 12; paragraph 124	Paragraph 124 goes beyond CRD IV (Article 76(5)), under which only the removal of the head of risk management is subject to approval by the management body in its supervisory function. In some cases, institutions do not have a head of the internal compliance function; rather, the responsibilities are distributed among several functions. There are also concerns about the information to be given to competent authorities about the removal of a head of an internal control function.	It is appropriate to ensure the same level of protection of the heads of internal control functions to ensure their independence, as is provided for in the Directive with respect to the head of risk management. If there is not a head of compliance, the guidelines apply to the person who leads the compliance function in parallel with his or her other function (e.g. head of legal). The information to be provided to the competent authority aims to ensure compliance with the requirements. However, the notification needs to respect applicable data protection laws.	No change.
Section 12; paragraph 125(c)	Some respondents affirm that in practice the supervisory authorities often require that the internal control functions should be subordinate to the CEO, so it is recommended that this section be clarified. Some respondents suggest that the guidelines should not attempt to give a definition of 'independent'.	The guidelines apply to all governance structures. The CEO is a person directing the business and therefore falls under the definition of 'management body'. The control functions may report directly to the CEO. The independence of control functions is a key feature that ensures that they can act effectively. Internal control functions should be able to report directly to the management body and the heads of control functions should have, where necessary, direct access to the management body in its supervisory function.	No change.
Paragraph 126	One respondent is strongly opposed to combining the risk management and compliance functions because of possible conflicts of interest.	Both functions form the second line of defence; therefore, the combination of those functions might be possible in some cases, taking into account the principle of proportionality.	No change.
Question 6 Paragraph 128	If an institution outsources the operational tasks of the internal control function, the institution should not have to maintain responsibility for this function within the institution; rather, it should be able to verify and ensure	The management body has overall responsibility for the institution's activities both outsourced and not outsourced, within the group and outside the group.	No change.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	that the outsourced activities are properly managed. One respondent suggests that a distinction should be drawn between intragroup outsourcing and outsourcing to third parties.		
Question 6 Paragraph 129	In paragraph 129, the concepts of internal control functions and institutions are confused. The paragraph should be rewritten.	The comment has been accommodated.	Paragraph 129 amended.
Question 6 Paragraphs 130 and 132	Paragraphs 130 and 132 seem to regulate the same issues and should be merged.	The comment has been accommodated.	Paragraph 130 amended, paragraph 132 deleted.
Question 6 Paragraph 134	The EBA should elaborate on which function in the institution should conduct the independent internal review of the risk management framework.	The review is typically conducted by the internal audit function.	Paragraph 134 amended.
Question 6	It would be desirable if all the requirements regarding the new product process could be included in the same section; see, for example, paragraphs 158-160 regarding risk and paragraph 181 regarding compliance.	The guidelines specify the tasks of the functions within this process, while Section 14 outlines the core procedural elements. The separation avoids redundancy within the guidelines.	No change.
Paragraph 141	It is considered that it creates too much of an administrative burden to require the approval of the management body to be sought with regard to not only the risk management framework but every individual detail of and change to it.	The comment has been accommodated	Paragraph 141 amended.
Section 14; paragraph 143	The section should better differentiate between new product approval and the process for material changes.	It has been clarified what material changes are and that the management body is responsible for approving the policy.	Section amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Some respondents point out that the paragraph implies that the management body should assess separate products, which is too far reaching. The management body should rather take into account changes to the product range when revisiting its strategies.		
Question 6 Paragraphs 144, 145 and 148	Some respondents point out that a shared responsibility between the compliance function and the risk management function could create overlap or that issues might fall in between. An institution should be able to assign the main responsibility to one of the functions, either risk or compliance.	It is the responsibility of the compliance function to monitor and ensure compliance with internal and external requirements. This may be done together with the risk management function. In addition, an independent review of the process will be done by the internal audit function. The paragraph has been removed from Section 14; the responsibilities are defined in the section on the internal control functions. Within the requirements set by the guidelines, institutions should define the internal responsibilities.	
Question 6 Paragraph 145	One respondent points out that, instead of a written opinion from the head of compliance, sufficient documentation by the compliance function would be sufficient. To require an approval would be too far reaching, as this mixes responsibilities between the first and second lines of defence.	The comment has been accommodated.	Paragraph 145 amended.
Paragraph 148	The wording 'under a variety of scenarios' goes too far and should be deleted.	The same wording was included in the previous guidelines.	No change.
Paragraph 150	A direct reporting line from the head of the risk management function to the supervisory board is not in line with national company laws.	The requirement is in line with Article 76(5) of Directive 2013/36/EU.	No change.
Question 6	One respondent asks whether the change from risk control function (GL 44) to risk management function	The wording follows the wording used in Directive 2013/36/EU.	Background section

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Section 15.1	has any meaning	The change has been explained in the background section.	amended.
Paragraphs 154, 161 and 164	The term 'all risks' should be understood as 'all significant risks'.	Institutions have to manage all their risks. The intensity is determined following a risk-based approach.	No change.
Question 6 Paragraph 156	It is unclear how the RMF would 'test' the robustness and sustainability of the risk strategy and appetite.	The wording has been clarified.	Paragraph 156 amended.
Question 6 Paragraph 158	'Material changes' should be clarified. In the respondent's view, such changes should be only those that have a material impact on the risk profile.	Paragraph 160 explains sufficiently the nature of material changes. The guidelines have been restructured and the section on material changes has been moved to Section 18, 'New products and significant changes'.	No change.
Paragraph 168	Some respondents suggest that the wording 'in its supervisory function' should be deleted, in order to make the paragraph applicable to their legal system, where the RMF reports directly only to the management body in its management function.	In line with Article 76(5) of Directive 2013/36/EU, there must be the possibility for the risk management function to report, where necessary, directly to the supervisory function.	No change.
Paragraph 172	It should be clarified if the head of the risk management function is equivalent to the CRO and if this role should be positioned at the CEO level in the case of significant institutions.	A definition of the term 'CRO' was not seen as necessary, as it is not used in the guidelines. The head of the risk management function does not necessarily have to be a member of the management body.	No change.
Section 15; paragraph 174	Respondents propose changing 'procedures' to 'processes'.	The comment has been accommodated.	Paragraph 174 amended.
Paragraphs 175-182	In smaller and less complex institutions it should be possible – as under the current guidelines – to combine the compliance function with other functions (e.g. HR, legal).	The guidelines specifically allow for such a combination. The text has been clarified further.	Section 15.2. amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Section 15; paragraph 179	Respondents propose reflecting existing laws in all Member States. In line with the response on paragraph 72, respondents consider that the definition of the roles and responsibilities of the compliance function might conflict with the definitions already in place in Member States.	The guidelines set out the expected role of the compliance function. The requirements regarding the organisation of the function have been further clarified. Other parts of the guidelines have been amended to stress that compliance is also a responsibility of the first line of defence.	Section 15.2. revised.
Question 6 Paragraph 179	Several respondents emphasise that the compliance function is not a legal advisor (this is the role of the legal department); rather, it ensures that the institution complies with laws and internal procedures.	The comment has been accommodated. The compliance function provides advice on how to deal with compliance issues.	Paragraph 179 amended.
Paragraph 180	The requirement to have a compliance policy and monitoring programme should not apply to small institutions. Smaller institutions should have standards or policies only for the most relevant areas, e.g. trading, anti-money laundering, data protection.	In general, small and less complex institutions may have policies that are less sophisticated than the policies of large and complex institutions. A compliance policy will include, inter alia and taking into account the business model of the institution, the areas mentioned by the respondent.	No change.
Paragraphs 180 and 181	Two respondents are concerned about the proposed cooperation between the risk management and the compliance functions. Such a requirement goes too far in their opinion.	Non-compliance with internal and external standards can have a material impact on an institution's risk profile; close cooperation between those functions is therefore needed and usually established in practice.	No change.
Section 15.3	Further more specific guidelines should be provided on when the audit function meets the requirements; the reference to size, nature and complexity is not sufficiently clear.	The principle of proportionality applies to all requirements and requires a case-by-case assessment.	No change.
Question 6 Section 15.3	Some respondents suggest that all items related to the internal audit should be in the same section and that audits should be done following a risk-based approach.	The review, its frequency and intensity should be done following a risk-based approach. The section deals with the requirements regarding the internal	Paragraph 185 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
General comment		audit function. However, sometimes this function is also relevant in different contexts and therefore requirements could not be further concentrated without creating significant repetition.	
Paragraph 186	The IAF should ensure that each *material* entity in the group falls within the scope of the IAF, and not each entity, in order to be risk-oriented.	All group entities should be subject to review by the internal audit function. The review, its frequency and intensity should be done following a risk-based approach.	No change.
Paragraphs 185, 186 and 187	The wording is not in line with the BCBS principles (principles 6 and 7) or audit standards. Some respondents suggest that more detail should be provided on the internal audit function's tasks.	The guidelines take into account the BCBS principles, but do not replicate them. In practice, institutions will also rely on other accepted internal audit standards. More detailed guidelines would risk being incompatible with such standards.	No change.
Paragraph 189	For the parent company of the group, the IAF does not have automatic access to the minutes of the management body in its supervisory function.	The guidelines do not require automated access via, for example, IT systems, but they do require that the internal audit function has access to such documents as needed to perform its tasks.	No change.
Paragraph 192	A few respondents point out that in some Member States the management body in its supervisory function is informed about the audit plan and can make comments on it but has no right to approve it.	The comment has been accommodated.	Paragraph 192 amended.
Question 6 Paragraph 196	Respondents comment that it is not clear if the paragraph refers to the first line or the second line of defence and ask why the advanced measurement approach (AMA) is included, since in future it will no longer be applicable.	The reference to the AMA has been moved to a footnote; the relevant parts of the regulation are still in force. The requirements apply to the institution; business continuity measures are needed also in the business lines. In large institutions, often a specific unit is created. Otherwise, this function can, for example, be part of the risk management function.	Paragraph 196 amended.
Question 7 Paragraph 202	A few respondents consider the listed topics to be included in the annual publication that can be required by competent authorities under Article 106(2) of	The comments have been accommodated; points (d) and (e) have been deleted.	Paragraph 202 amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Directive 2013/36/EU as too far reaching. Paragraph 202(d): several respondents deem it inappropriate to publish an overview of material outsourcing of activities, processes and systems, as this could jeopardise business secrecy. The same applies to paragraph 202(e), dealing with close links with other natural or legal persons.		
Question 8 Annex I	Some respondents point out that the criteria listed in Annex I do not allow institutions sufficient discretion to take into account their special features and do not sufficiently take into account national legal frameworks. Some respondents consider that points 6(c) and (d) are not appropriate: either they should be deleted, as they are part of the audit process, or it should be clarified that they refer to the overall handling of weaknesses identified and measures to manage them, and not to each individual case.	The guidelines aim to harmonise the documentation of governance policies and arrangements, which should also reduce the burden for institutions active in multiple Member States. Points 6(c) and (d) have been deleted.	Annex I amended.
Question 8 Costs of the guidelines	Respondents find it difficult to assess and estimate the costs that the guidelines will incur, especially because there remains some uncertainty as regards the application of the principle of proportionality and the level of application of the guidelines. According to respondents, costs would be significant if the guidelines were to be applied to each subsidiary/entity on an individual basis. Costs would be driven by the requirements to develop, adopt, implement, monitor and assess new policies and procedures. For instance, the requirement related to the development of ethical standards for external	The impact assessment has been updated. Costs caused by the provisions of Directive 2013/36/EU directly (e.g. regarding the scope of application) are not taken into consideration in the assessment of the impact caused by the guidelines.	Impact assessment amended.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	services providers is deemed to be costly and to provide limited added value: one respondent believes that, when these providers already have a code of ethics and business conduct, financial institutions should not have additional obligations in this respect. Overall, the administrative burden caused by the guidelines would be non-negligible. More specifically, respondents have identified the following costs: the need to recruit additional staff to comply with the guidelines and inefficient allocation of managers' time. According to some respondents, both EU groups and subsidiaries of EU groups involved in non-regulated activities or activities regulated to a low degree would be penalised by those costs and suffer from a non-level playing field with non-EU groups and non-EU entities involved in non-regulated activities or activities regulated to a low degree, as these entities are supposed to apply lighter requirements in the field of corporate governance.		