EBA/CP/2016/16

28/10/2016

Consultation Paper

Draft Guidelines on internal governance

Contents

Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2. [*The part of the phrase from 'and in particular' onwards to be added* only *if, as the case may be, specific questions are provided in the CP*].

Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 28.01.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

Executive Summary

In recent years, internal governance issues have received increasing attention from various international bodies. Their main effort has been to correct the institutions' weak or superficial internal governance practices as identified in the financial crisis. Recently more focus was given to conduct-related shortcomings and activities in financial offshore centers.

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 and the importance of a strong supervisory function that challenges management decision-making and the setting and implementation of sound risk strategies and risk management frameworks.

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 EBA is mandated by Article 74 of Directive 2013/36/EU to develop Guidelines in this area.

The draft 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, the organisation of institutions and groups, including the need to create transparent structures that allow for a supervision of all their activities and specifies requirements for the three lines of defense and, in particular, the risk management, compliance and audit function.

The draft Guidelines update the existing set of Guidelines on internal governance and, in particular, introduce additional aspects that aim to foster a sound risk culture to be implemented by the management body, to strengthen its oversight over the institutions' activities and their risk management framework. Additional guidelines have been provided to further increase the transparency of institutions' offshore activities and the consideration of risks within institutions' change processes.

Next steps

The European Banking Authority (EBA) will finalise these Guidelines following the public consultation. The existing Guidelines on internal governance, published on 27 September 2011, will be repealed when the revised Guidelines enter into force. The EBA is updating in parallel its Guidelines on the assessment of the suitability of the members of the management body and key function holders.

Background

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, are to operate well.

2. In recent years, internal governance issues have received the increasing attention of various international bodies. Their main effort has been to correct the institutions' weak or superficial internal governance practices as identified in 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, more focus was given to conduct-related shortcomings and activities in financial offshore centers.

3. In some cases, 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 was also identified. The management body, both in its management, but especially in its supervisory function, might not have understood the complexity of their business and the risks involved, and consequently failed to identify and constrain excessive risk-taking in an effective manner.

4. The internal control frameworks, including risk management, were often not sufficiently integrated within institutions or groups. A uniform methodology and terminology was missing, and, therefore, there was no holistic view of all risks. Internal control functions often lacked appropriate resources, status and/or expertise.

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

6. Against this background, there is clear need to address the potentially detrimental effect of poorly designed internal governance arrangements on the sound management of risk to ensure effective oversight by the management body, promote a sound risk culture at all levels of institutions and 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 that institutions shall 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 the risk management, the setting up of a risk committee for significant institutions and the organisation of the risk management function.

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 of a nomination committee for significant institutions.

11. Article 109 (2) of the Directive 2013/36/EU requires parent undertakings and subsidiaries subject to this Directive to meet the governance requirements 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, i competent authorities should ensure that parent undertakings and subsidiaries subject to this Directive implement such arrangements, processes and mechanisms in their subsidiaries not subject to this Directive. Those arrangements, processes and mechanisms shall also be consistent and well-integrated and those subsidiaries shall also be able to produce any data and information relevant to the purpose of supervision.

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

13. 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 as applicable to institutions within Member States where the branch is located, taking into account specific internal governance arrangements, e.g. that they do not have a management body but persons that are responsible for effectively direct the business.

14. 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 suitability of the members of the management and key function holders. The existing Guidelines on internal governance, published on 27 September 2011, will be repealed when the revised Guidelines enter into force.

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

Rationale and objective of the guidelines

16. 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.

17. Directive 2013/36/EU (CRD IV) sets out requirements aiming at remedying weaknesses that were identified during the financial crisis regarding internal governance arrangements, including effective oversight by the management body, authority, stature, resources and accessibility and in particular the sound management of risks.

18. 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 corporate governance principles for banks of the Basel Committee for Banking Supervision[1].

19. Member States company law usually provides for either a unitary and/or a dual board structure; the Guidelines apply to both structures. The Guidelines do not advocate any particular structure and are intended to embrace all existing governance structures. The management body in its management function sets the direction for the institution and is responsible 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 role includes reviewing the performance of the management function and the achievement of objectives, and ensuring the integrity of financial information as well as the soundness and effectiveness of the risk management and internal controls.

20. The Guidelines take into account the so-called "three lines of defence" model to identify the functions within institutions responsible to address and manage the risks. The business line – the first line of defence – takes and manages the risks that it incurs in conducting its activities. The independent risk management and compliance functions, as a second line of defence are responsible for further identifying, measuring, monitoring, and reporting risks and ensuring compliance with internal and external requirements on an individual and consolidated basis, of all business lines and internal units, independently from the first line of defence. The independent internal audit function as the third line of defence, conducts risk-based and general audits and reviews that the internal governance arrangements,

[1] The BCBS guidelines can be found under the following link: http://www.bis.org/bcbs/publ/d328.htm

processes and mechanisms are sound and effective, are implemented and consistently applied. The internal audit function is also in charge of the independent review of the first two 'lines of defence'. Within the three lines of defence, appropriate internal control procedures, mechanisms and procedures should be designed, developed, maintained and evaluated by the management body. To ensure their proper functioning, all internal control functions need to have the highest level of independence of the business they control and have the appropriate financial and human resources to perform their tasks.

21. The Guidelines specify requirements of Directive 2013/36/EU that need to be considered when setting up new structures, e.g. in offshore financial centres, that 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 such structures.

22. The Guidelines aim to establish a strong risk culture in institutions. Risks should be taken within a well-defined framework for the institutions' risk strategy and appetite. This includes the setting of a system of limits and controls. Risks within new business areas, but also risks that may result from changes to institutions products, processes and systems are to be duly identified, assessed, managed and monitored. The risk management function should be involved in the setting of the framework and the approval of such changes.

23. To improve the decision-making and to ensure compliance with the institutions' strategies and risk limits, institutions should implement a conflict of interest policy and internal whistleblowing procedures.

EBA/GL-REC/2016/XX

DD Month YYYY

Draft Guidelines

on internal governance

Compliance and reporting obligations

Status of these guidelines

1. These guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010[2]. 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/2016/xx'. 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.

[2] 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).

Subject matter, scope and definitions

Subject matter

6. 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[3] to ensure effective and prudent management of the institution.

Addressee

7. These guidelines are addressed to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) 575/2013[4], 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) 575/2013.

Scope of application

8. These guidelines apply in relation to institutions' governance arrangements, including their organisational structure with 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.

9. Member States usually use one of two governance structures - a unitary or a dual board structure. In both structures the management body in its management function and the management body in its supervisory function each play their own role in the management of the institution, directly and when established with the assistance of committees. In Member States where the national legislation within a Member State does not distinguish between the management and supervisory functions of the management body, references to the supervisory function should be understood as applying to the management body which is responsible for that function according to national law.

10. For the purposes of these guidelines, any reference to the members of the management body or to the members of the management body in its management function should be understood as applying also to the Chief Executive Officer (CEO), as defined in these guidelines, even if he or she has not been proposed or appointed as a formal member of the

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

[4] 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).

management body. Likewise, any reference to the management body or to the management body in its management function should be understood as including the CEO.

11. The definitions of Chief Executive Officer (CEO) and Chief Financial Officer (CFO) used in these guidelines are purely functional and not intended to impose the appointment of those officers or creation of such positions unless prescribed by relevant EU or national law.

12. Institutions should comply and competent authorities should ensure that those 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

13. 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, risk management and control capabilities as well as its regulatory constraints.
Risk culture	means institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and 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) 575/2013.
Staff	means all employees of an institution and its subsidiaries, including subsidiaries not subject to Directive 2013/36/EU, and all members of their respective management bodies.
Chief Executive Officer (CEO)	means the person who is responsible for managing and providing steer to manage the overall business activities of an institution.
Chief Financial Officer (CFO)	means the person that is primarily responsible for managing the financial resources and risks, financial planning and reporting and record-keeping.
Heads of internal control	means the persons at the highest hierarchical level in charge of effectively managing the day to day operation of the risk

functions	management, compliance and audit functions.
Key function holders	means the persons who have significant influence over the direction of the institution, but who are not members of the management body nor 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 (EEA)/European Free Trade Association (EFTA) 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) 575/20132 on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) 575/2013. The prudential consolidation includes all subsidiaries that are institutions or financial institutions, as defined in Article 4(3) and (26), respectively, of Regulation (EU) 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 which 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) 575/2013.
Significant institutions	means institutions referred to in Article 131 of Directive 2013/36/EU (global systemically important institutions or 'G-SIIs', and other systemically important institutions or 'O-SIIs'), and, as appropriate, other institutions determined by the competent authority, based on an assessment of the institutions' size, internal organisation and the nature, the scope and the complexity of their activities.
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.
Conflict of interest	means a situation of conflict between the duty of a person and private interests of an individual, which could improperly influence the performance of his or her duties and responsibilities.
Directorship	means a position as a member of the management body of an institution or another legal entity.

Implementation

Date of application

14. These guidelines apply from dd.mm.yyyy

Repeal

15. The EBA guidelines on internal governance (GL 44) of 27 September 2011 are repealed with effect from [date].

Q1: Are the guidelines regarding the subject matter, scope, definitions and implementation appropriate and sufficiently clear?

Draft guidelines

Title I - Role of the management body regarding internal governance

1 Duties and responsibilities of the management body

16. In accordance with Article 88(1) of Directive 2013/36/EU, the management body must have the 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.

17. The duties of the management body should be clearly defined distinguishing between the members of the management body in its management function (executive members) and members of the management body in its supervisory function (non-executive members). The responsibilities and duties of the management body should be described in a written document and duly approved by the management body in its supervisory function.

18. The management body in its supervisory function and management function should interact effectively. Both functions should provide each other with sufficient information to allow them to perform their respective roles'.

19. 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 its risk appetite and its risk management framework and measures to ensure that the management body devotes sufficient time to risk issues;

c. an adequate, effective and independent internal control framework, that includes a clear organisational structure and a well-functioning risk management, compliance and internal 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. 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 Article 74 (3) of Directive 2013/36/EU;

f. arrangements aimed at ensuring that the individual and collective suitability assessment of the management body is carried out effectively, the composition and the succession planning of the management body is appropriate and the management body performs its functions effectively[5];

g. a selection and suitability assessment process for key function holders[6];

h. arrangements aimed at ensuring the internal functioning of each committee of the management body in its supervisory function, when established, detailing the role, composition and tasks of each of them (including minutes of the discussions and of the decisions taken), including appropriate information flow and reporting lines between the management body in its supervisory function and each committee, when established, competent authorities and other interested parties;

i. a risk culture in line with Section 9.1 of these guidelines, which addresses the institution’s risk awareness and risk-taking behaviour;

j. a corporate culture and values that foster responsible and ethical behaviour, including a code of conduct or similar instrument; and

[5] See also CP on EBA Guidelines on the suitability of members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA’s website.

[6] See also CP on EBA Guidelines on the suitability of members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA’s website

k. 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;

20. The management body must oversee the process of disclosure and communications.

21. 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.

22. The management body should monitor and periodically review and address any weaknesses identified regarding the implementation of processes, strategies and policies related to the responsibilities listed in paragraphs 18 to 19. The internal governance framework and its implementation should be reviewed and updated on a periodical basis taking into account the proportionality principle as further developed in Title III. A deeper review should be carried out in case of material changes affecting the institution.

2 Supervisory function of the management body

23. The management body in its supervisory function should monitor and constructively challenge the strategy of the institution, management actions and decisions and perform their role independently from the management body in its management function. The management body in its supervisory function should oversee the management body in its management function by monitoring and scrutinising its performance and the implementation of the institution's strategy and objectives in line with the strategy and objectives that have been defined and approved by the former. The management body in its supervisory function should also ensure the integrity of the financial information and reporting, and internal control framework, including effective and sound risk management.

24. The management body in its supervisory function should:

a. have suitable members [7] who do not perform any executive function [8] in the institution and are able to fully understand and oversee the risk strategy and the risk appetite of the institution;

b. taking into account the proportionality principle as further developed in Title III, appropriately fulfill the duties and role of the risk committee, the remuneration committee and the nomination committee, respectively, where no such committees have been set up;

[7] See also CP on EBA Guidelines on the suitability of members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA's website

[8] For this purpose "executive function" should not be understood including employee representative

c. provide effective oversight of the management body in its management function, including reviewing its individual and collective performance;

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

e. oversee and monitor that the institution's strategic objectives, organisational structure, risk strategy and policy as well as other policies such as remuneration and disclosure are implemented consistently;

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

g. ensure that the heads of internal control functions are able to act independently and, without prejudice to report to other internal bodies, can raise concerns and warn the management body in its supervisory function directly, where appropriate, when adverse risk developments affect or may affect the institution;

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

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

j. oversee the implementation and maintenance of effective policies to identify, manage and mitigate actual and potential conflicts of interest.

3 Role of the chair of the management body

25. The chair of the management body should lead the management body and be responsible for its effective overall functioning.

26. 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.

27. As a general principle, the chair of the management body in its supervisory function should be an independent or 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, a senior independent board member or having a larger number of non-executives 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 the

supervisory function and the CEO of an institution must not be the same person, unless justified by the institution and authorized by the competent authority.

28. The chair should set the meeting agenda 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 documents and information should be received with enough time before the meeting to enable the management body to take informed decisions.

29. The chair of the management body should contribute to ensure clear allocation of responsibilities between executive and non-executive 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 participate in the discussions and to cast their vote with awareness.

4 Management function of the management body

30. 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.

31. 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.

32. The management body in its management function should constructively challenge and review critically propositions, explanations and information received when exercising its judgement and taking decisions. Its decision-making should not be dominated by a member or a small set of members.

33. The management body in its management function should comprehensively report and inform regularly and without delay, the management body in its supervisory function of the relevant elements for the assessment of a situation, the risks 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.

Member State company law usually provides for a unitary and/or a dual board structure; the guidelines apply to both structures. The guidelines do not advocate any particular structure and are intended to embrace all existing governance structures. The management body in its management function sets the direction for the institution and is responsible for the day-to-day running of the institution. The management body in its supervisory function oversees and challenges the management body in its management function and provides appropriate advice. This oversight role includes reviewing the performance of the management body in its management function, its decision-making and the achievement of objectives, and

ensuring the integrity of financial information as well as sound and effective risk management and internal controls.

The draft Guidelines set out the duties and responsibilities of the management body in 3 sections. In the first the responsibilities of the management body are set out. In a 2-tier system these responsibilities might be assigned in some cases to the management or the supervisory function of the management body in line with applicable company law. The second section sets out the requirements regarding the supervisory function and the final section the requirements of the management function. However, in a 1-tier structure the responsibilities of the management body are executed collectively by all members. Despite the overall responsibility of all members certain aspects are the prior responsibility of the members in the management function and other aspects the prior responsibility of the supervisory function, those aspects have been assigned accordingly in the present Consultation Paper.

Q2: Are there any conflicts between the responsibilities assigned by national company law to a specific function of the management body and the responsibilities assigned by the Guidelines, in particular within paragraph 23, to either the management or supervisory function?

5 Specialised committees of the management body in its supervisory function [9]

5.1 Setting up committees

34. In accordance with Article 109 of Directive 2013/36/EU in conjunction with Articles 76 (3) and 88(2) of Directive 2013/36/EU, all institutions which are themselves significant, considering the individual, parent company and group level, must establish a risk and a nomination[10] committee to advise the management body in its supervisory function and to prepare the decisions to be taken by this body.

35. Where no risk or nomination committee is established, the references in these guidelines to those committees should be construed as applying to the supervisory function taking into account the principle of proportionality as further developed in Title III.

36. Significant institutions may, taking into account the criteria described in Title III of these guidelines, establish other specialised committees (e.g. ethics, conduct and compliance

[9] With regard to the remuneration committee under article 95 of Directive 2013/36/EU please refer to the guidelines on sound remuneration policies. For the role of the nomination committee under article 88 (2) of Directive 2013/36/EU please refer to the guidelines on the suitability of members of the management body and key function holders. Both documents are available under: www.eba.europa.eu.

[10] See also CP on EBA Guidelines on the suitability of members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA's website

committee). Institutions that are not significant may also consider setting up such committees.

37. Specialised committees should regularly report to the management body in its supervisory function. Specialised committees should interact with each other as appropriate. Such interaction could be done through cross-participation: the chair or a member of a specialised committee might also be a member of another specialised committee. However, taking into account the size of the management body and the number of independent members of the management body in its supervisory function, institutions should ensure that committees are not being composed mostly of the same group of members which form another committee.

38. 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.

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

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

41. Committees should document the agenda of committee meetings and their main conclusions.

5.2 Composition of committees[11]

42. The risk and nomination committees should be composed of members of the management body in its supervisory function who do not perform executive functions in the institution concerned. Further, the specialised committees should be composed of a sufficient number of independent[12] members to be able to ensure that they can perform their duties in an effective manner. In particular, the risk committee should include a majority of members who are independent. Where there are not a sufficient number of qualified independent members, institutions should implement other measures to limit conflicts of interest in decisions related to risk management and nomination.

43. Members of the risk committee should have individually and collectively appropriate knowledge, skills, expertise and professional experience concerning risk management, and

[11] This section should be read in conjunction with the CP on guidelines on the assessment of suitability of the members of the management body and key function holders

[12] See also CP on EBA Guidelines on the suitability of members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA's website

control practices. The same applies to members of the nomination committee regarding selection process, suitability and control practices and the audit committee, where established, regarding audit processes and practices.

44. Each committee should have a chair that is an independent[13] member of the management body in its supervisory function. Members of the management body in its supervisory function should not chair as a general principle multiple committees unless this is justified taking into account the overall composition and experience, knowledge and skills of the management body. Institutions should consider, the occasional rotation of chairs and members of committees taking into account the specific experience, knowledge, skills which are individually or collectively required for certain committees.

45. Without prejudice to Directive 2006/43/EC[14], where an audit committee is established, a majority of the members of the audit committee should be independent of the audited institution. The chairman of the audit committee should also be independent of the audited institution.

5.3 Committees' processes

46. The risk and nomination committees should at least:

    a. have access to all relevant information and data including access to information and data where appropriate access to information and data from relevant corporate and control function (e.g. legal, finance, human resources, IT, risk, compliance, audit etc.);

    b. receive regular reporting, ad-hoc information, communications or opinions from heads of internal control functions concerning the current risk profile of the institution, risk culture, risk limits and of any breaches that may have occurred and 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;

    d. ensure the proper involvement of the internal control functions and other relevant functions within the respective areas of expertise and, where necessary, seek external expert advice.

[13] See CP on guidelines on the assessment of suitability of the members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA's website

[14] 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 amended by Directive 2014/56/EU.

5.4 Role of the risk committee

47. Where established, the risk committee should:

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

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

    c. oversee the implementation of the strategies for capital and liquidity management as well as for all the remaining relevant risks of an institution, such as market, credit, operational, reputational and information technology 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 of the risk strategy resulting from inter alia changes in the business model of the institution or market developments or from recommendation made by the risk management function;

    e. review the proposed 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 reacts to external and internal events;

    g. examine the alignment between all financial products and services offered to clients and the business model as well as the risk strategy of the institution. The risk committee should assess the risks associated with the offered financial products and services and examine the alignment with the prices assigned and profits gained from those products and services.

48. The risk committee should collaborate with other committees of the supervisory function 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.

49. 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, liquidity and the likelihood and timing of earnings. The management body members of the risk committee should be able to participate in the meetings of the remuneration committee, where both committees are established, and vice versa.

5.5 Role of the audit committee

50. In accordance with Directive 2006/43/EC[15], where established, the audit committee should, inter alia:

    a. monitor the effectiveness of the institution's internal quality control and risk management systems and, where applicable, its internal audit, regarding the financial reporting of the audited institution;

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

    c. monitor the financial reporting process and submit recommendations or proposals to ensure its integrity;

    d. review and monitor the independence of the statutory auditors or the audit firms, and in particular the appropriateness of the provision of non-audit services to the audited institution;

    e. monitor the statutory audit of the annual and consolidated financial statements;

    f. be responsible for the procedure for the selection of external statutory auditor(s) or the audit firm(s) and recommend for approval by to the institution's competent body their appointment, compensation and dismissal;

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

    h. review audit reports.

5.6 Combined risk/audit committee

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

52. 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[16].

[15] 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 amended by Directive 2014/56/EU

[16] See also CP on EBA Guidelines on the suitability of members of the management body and key function holders that has been published in parallel with this consultation paper on the EBA's website

6 Organisational framework and structure

6.1 Organisational framework

53. The management body of an institution should ensure a suitable and transparent organisational and operational structure for that institution and should have a written, clear and detailed description of it. The structure should promote and demonstrate the effective and prudent management of an institution at individual, sub-consolidated and consolidated level. The management body should ensure the highest level of independence of the internal control functions 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 within an institution should be clear, well-defined, coherent, enforceable and duly documented.

54. All members of the management body should be fully aware of the structure of the management body, the division of tasks and responsibilities within the management body, its committees, and within the institution, in particular among key function holders.

55. The management body should assess how the various elements of the organisational and operational structure complement and interact with each other. The structure should not impede the ability of the management body to oversee and manage effectively the risks the institution or the group faces and of the competent authority to effectively supervise the institution.

56. The management body should assess whether and how changes to the groups 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

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

58. 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, particularly 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 section 8 of these guidelines, are clear,

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

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

60. The management body of a consolidating institution should understand not only the legal and organisational 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, intra-group exposures and 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 organizational chart and ownership structure and businesses of each legal entity and that the institutions within the group comply with all supervisory reporting requirements.

61. The management body of a consolidating institution should ensure the different group entities (including the institution itself) receive enough information for all of them to get a clear perception of the general objectives, strategies and risk profile of the group. Any flow of significant information between entities relevant to the group's operational functioning should be documented and made available promptly, when requested, to the management body, the internal control functions and competent authorities, as appropriate.

62. 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 section 8 of the guidelines. This includes:

    a. information on major risk drivers;

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

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

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

63. Institutions should avoid setting up complex and potentially non-transparent structures. Institutions should base their decision on a risk assessment to identify whether these

structures may be used for a purpose connected with money laundering or other financial crimes[17]. 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 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 to set up a structure gives rise to concern; and

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.

64. In any case, institutions should not set up opaque or unnecessarily complex structures that have no clear economic rationale or legal purpose or where they are not satisfied that these structures will not be used for a purpose connected with financial crime.

65. When setting up such structures, the management body should understand them and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. Such structures should only be approved and maintained when their purpose has been clearly defined and understood, 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 organizational and operational structures, and the greater the risks, the more intensive the oversight of the structures should be.

66. Institutions should document their decision and be able to justify their decision to competent authorities.

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

[17] For further details on the assessment of country risk and the risk associated with individual products and customers, institutions should refer also to the CP on 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

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 operational structure, its risk profile and its reputational risk;

b. information concerning these activities and risks thereof is accessible to the consolidating institution, 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.

68. 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 form vehicles in offshore jurisdictions; developing complex structures and finance transactions for them or providing trustee services) which pose similar internal governance challenges and create significant operational and reputational risks. In particular, institutions should analyse the purpose why a client wants to set up a particular structure.

69. All these structures and activities, including their compliance with legislation and professional standards, should be subject to regular review by the internal audit function.

Q3: Are the guidelines in Title I regarding the role of the management body appropriate and sufficiently clear?

Title II - Internal governance policy, risk culture and business conduct

7 Internal governance policy

70. The management body should define, adopt and maintain a governance policy to implement a clear organisational and operational structure with well-defined, transparent and consistent lines of responsibility taking into account the aspects set out in Annex I of these guidelines. The management body in its management function is responsible for the implementation of that policy. The management body in its supervisory function is responsible for overseeing its implementation and that it is fully operating as intended and should ensure that the institution's policy is aligned with the institution's overall internal governance arrangements, corporate culture and risk appetite.

71. The policy should be clear, well documented and transparent. When developing the policy, the management body may request and take into account input from other internal committees, in particular the risk, remuneration and nomination committees where

established and corporate functions, e.g. the legal, human resources function or internal control functions.

72. Internal control functions should provide effective input in accordance with their roles regarding the policy. Notably, the compliance function should analyse how the 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.

73. The management body in its supervisory function should monitor the effects of the policy and carry out a periodical review of the design, implementation and effectiveness of the governance policy taking into account the recommendation from the relevant internal committees, when established, and the internal audit function. Where appropriate, policy should be amended.

74. Any changes to the governance policy should also be duly approved by the management body. Documentation regarding the adoption of the policy and any amendments thereof (e.g. minutes of relevant meetings) should be maintained and communicated, where appropriate, to the competent authority particularly in case of significant changes.

8 Governance policy in a group context

75. In accordance with Article 109 of Directive 2013/36/EU, the consolidating institution should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated and sub consolidated basis. To this end all subsidiaries within the scope of prudential consolidation, including those not subject to Directive 2013/36/EU, should implement such arrangements, processes and mechanisms. Competent functions within the consolidating institution and its subsidiaries should interact and exchange information as appropriate. The governance arrangements, processes and mechanisms should ensure that the consolidating institution has sufficient information and is able to assess the group wide risk profile, as further detailed in paragraphs 56 to 58.

76. At the consolidated or sub-consolidated level, the consolidating institution and competent authorities should ensure that a group-wide written internal governance policy describing arrangements, processes and mechanisms is implemented and complied with by all institutions and other entities within the scope of prudential consolidation, including their subsidiaries not subject to Directive 2013/36/EU. When implementing that policy the consolidating institution should ensure the implementation of robust governance arrangements in each subsidiary and consider specific arrangements, processes and mechanisms where business activities are not organised in separate legal entities, but within a matrix of business lines that encompasses multiple legal entities.

77. The consolidating institution should ensure that the institutions and entities within the group comply with all specific requirements in any relevant jurisdiction. Regarding

institutions and entities within a group located in more than one Member State, the consolidating institution should ensure that the group-wide policy takes into account differences between national company laws and other regulatory requirements.

78. The consolidating institution should ensure that subsidiaries established in third countries, that are included in the scope of prudential consolidation, have a policy that is consistent with the group-wide policy and complies with the requirements of Articles 74, 76 and 88 of Directive 2013/36/EU and these guidelines as long as this is not unlawful under the laws of the third country.

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

9 Framework for business conduct

9.1 Risk culture

80. 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.

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

82. Institutions should develop a risk culture through policies, communication and training of staff regarding the institutions' activities, strategy and risk profile and adapt the communication and training to staff considering their responsibilities regarding risk taking and risk management.

83. Staff of the institution 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, taking into account the institution's risk capacity/appetite and manage risk in line with the institution's policies, procedures and controls.

84. 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. Staff should act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance within or outside the institution. The management body should on on-going 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, its risk appetite and risk capacity. They should be capable of performing their roles and be aware that they are 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; and

d. Incentives: appropriate incentives should play a key role in aligning risk-taking behaviour to the institution's risk profile and its long term interest[18].

9.2 Corporate values and code of conduct

85. 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 ensure the implementation of such standards (e.g. a code of conduct) and compliance by staff. Equivalent ethical standards should be developed for external services providers. It should also oversee adherence to these standards by staff. These standards should be also taken into account for outsourcing activities.

86. The implemented standards should aim at reducing 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 the cost of fines, litigation costs, restrictions imposed by competent authorities and other financial and criminal penalties and the loss of brand value and consumer confidence.

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

[18] Please refer also to EBA guidelines on sound remuneration policies available under: https://www.eba.europa.eu/regulation-and-policy/remuneration

a. recall that all institutions' activities should be conducted in compliance with the applicable laws and with the institution's corporate values;

b. promote risk awareness through a strong risk culture in line with section 9.1 of the guidelines, conveying the management body's expectation that activities do not go beyond the defined risk appetite and limits defined by the institution and the respective responsibilities of staff;

c. define 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 the compliance with legal and regulatory requirements and internal policies, staff are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; and

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

88. Institutions should oversee the compliance with such standards and ensure the awareness of staff, e.g. by providing training. Institutions should define the function responsible for evaluating breaches of the code of conduct and a process for dealing with issues of non-compliance.

89. A regular review of the implementation and compliance with those ethical and professional standards should be performed. The results should periodically be reported to the management body.

9.3 Conflicts of interest[19]

90. The management body should be responsible for establishing and overseeing the implementation and maintenance of effective policies to identify, manage, address and mitigate actual and potential conflicts of interest of staff.

91. In particular, material conflict of interest at management body level, individually and collectively, should be adequately documented, communicated to, discussed and duly managed by the management body. Conflicts of interest that have been disclosed to and duly approved by the management body should be appropriately managed. Conflicts of interests caused by having mandates in competing institutions or other entities should be

[19] This section should be read in conjunction with the CP on guidelines on the assessment of the suitability of members of the management body and key function holders

prevented; this excludes mandates in institutions that belong to the same institutional protection scheme.

92. A duly approved written policy should identify the relationships, services, activities or transactions of an institution in which conflicts of interest may arise and should state how these conflicts should be managed. This policy should equally cover the conflict of interest risk specific to the management body in its supervisory function. In all circumstances the interest of the institution should be central in the decisions taken. This policy should cover at least relationships between an institution and:

    a. its qualifying shareholders;

    b. the members of its management body;

    c. its staff;

    d. material suppliers or business partners;

    e. other related parties (e.g. its parent company or subsidiaries); and

    f. legal or natural persons closely linked to persons under points (a) to (e) above.

93. A consolidating institution should consider the interests of all its subsidiaries, and how these interests contribute to the interest of the institution and interests of the group as a whole over the long term.

94. The conflict of interest policy should set out procedures and measures to be adopted to prevent, identify actual or potential conflicts of interest, assess their materiality, decide on mitigating measures and communicate any material actual or potential conflicts of interest of staff to the management body. Such procedures and measures should be documented and include:

    a. establishing adequate segregation of duties, e.g. entrusting conflicting activities within the chain of transactions or of services to different persons or entrusting supervisory and reporting responsibilities for conflicting activities to different persons;

    b. establishing information barriers such as physical separation of certain departments;

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

    d. establishing the staff's duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest;

e. establishing a member's responsibility to abstain from voting on any matter where the member 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;

f. establishing adequate procedures for transactions with related parties (e.g. requiring transactions to be conducted at arm's length; requiring that all relevant internal control procedures fully apply to such transactions; requiring a binding consultative advice by independent members of the management body; an approval by shareholders of the most relevant transactions; limits to the exposure of such transactions); and

g. preventing members of the management body from holding directorships in competing institutions.

95. If any conflict of interest is identified, the institution should issue a statement as to how this conflict has been satisfactorily mitigated or remedied including a reference to the relevant parts of the institution's conflicts of interest policy or any bespoke conflict management or mitigation arrangements.

9.4 Internal alert procedures

96. Institutions should put in place appropriate procedures for the staff to report potential or actual breaches of regulatory requirements, in particular national provisions transposing Directive 2013/36/EU and Regulation (EU) No 575/2013, and internal governance arrangements, through a specific, independent and autonomous channel. It should not be necessary that reporting staff has evidence of it, but a level of initial certainty that provides sufficient reason to launch an investigation.

97. To avoid conflicts of interest, reporting of breaches by staff should take place 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 personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach, in accordance with Directive 95/46/EC.

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

99. Information provided by the staff via the alert procedures should, if appropriate, be made available to the management body and other responsible functions; where required by the staff member reporting an incident the information should be provided to the management body and other responsible functions in an anonymised way. Institutions may also provide for a whistle blowing process that allows handling in information in an anonymised way.

100. Institutions should ensure that the person reporting breaches is appropriately protected from any negative impact, e.g. retaliation, discrimination or other types of unfair treatment.

The institution should ensure that no person under the institution's control engages in victimisation of staff who reported a breach and take appropriate measures against those responsible for any such victimisation.

101. Institutions should also protect persons that have been reported from any negative effect in case the investigation results in the fact that no evidence is found that justifies taking measures against that person.

102. In particular, internal alert procedures should:

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

b. provide clear rules that ensure that confidentiality is guaranteed in all cases in relation to the person who reports the breaches committed within the institution, unless disclosure is required by national law in the context of further investigations or subsequent judicial proceedings;

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

d. ensure that confirmation of receipt to staff who raised potential or actual breaches is provided;

e. ensure the tracking of the outcome of reported breaches;

f. ensure appropriate record keeping.

103. Institutions may also consider making a member of the management body in its supervisory function responsible for ensuring and overseeing the integrity, independence and effectiveness of the institution's internal alert policies and procedures, including those policies and procedures intended to protect staff that raise concerns from being victimised because they have disclosed reportable breaches.

10 Reporting of breaches to competent authorities

104. Competent authorities should establish effective and reliable mechanisms to encourage institutions' staff to report competent authorities on potential or actual breaches of regulatory requirements, in particular national provisions transposing Directive 2013/36/EU and of Regulation (EU) No 575/2013, and internal governance arrangements. These mechanisms should include at least:

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

b. appropriate protection referred to in section 9.4;

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

d. clear procedures as set out in paragraph 98.

105. Without prejudice to the possibility to report breaches via the competent authorities' mechanisms, competent authorities may encourage employees to first try and seek to use their institutions' internal alert procedures.

11 Outsourcing policy[20]

106. 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.

107. The outsourcing policy should consider the impact of outsourcing on an institution's business and the risks it faces (such as operational, reputational and concentration risk). 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). The policy should be reviewed and updated regularly, with appropriate changes implemented in a timely manner.

108. 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 an outsourcing does not relieve the institution of its regulatory obligations and its responsibilities to its customers.

109. 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 (e.g. by a separate legal entity within an institution's group) and take into account any specific group circumstances.

Q4: Are the guidelines in Title II regarding the internal governance policy, risk culture and business conduct appropriate and sufficiently clear?

[20] The present Guideline is limited to the general outsourcing policy; specific aspects of the issue of outsourcing are treated in the CEBS Guidelines on Outsourcing, available at EBA's website under https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing

Title III - Proportionality

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

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

112. 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 or the quantity of assets held by the institution or its subsidiaries within the scope of prudential consolidation;

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

c. the legal form and whether the institution is part of group and, if so, the proportionality assessment done 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. Internal Rating Based Approach);

f. the type of authorised activity and services (e.g. loans and deposits, investment banking);

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

h. the risk strategy, risk appetite and actual risk profile of the institution, take into account also the result of the annual capital adequacy assessment;

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

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

k. the outsourced activities and distribution channel;

l. the existing IT systems, including IT continuity systems and outsourcing activities in this area e.g. cloud computing.

Q5: Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear? When providing your answer please specify which aspects and the reasons why. In this respect, institutions are asked to provide quantitative and qualitative information about the size, internal organisation and the nature, scale and complexity of the activities of their institution to support their answers.

Title IV - Internal control framework

12 Internal control framework

113. Institutions should develop and maintain a strong and comprehensive internal control framework and a strong control culture that encourage a positive attitude towards control within the institution, including internal control functions with appropriate and sufficient authority, stature, and access to management body to fulfil their mission, and a risk management framework. The internal control functions should include a risk management function, a compliance function and an internal audit function. The risk management and compliance function should be subject to review by the internal audit function. The proportionality criteria listed in Title III of these guidelines should be taken into account when developing the internal control framework.

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

115. 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. 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.

12.1 Implementing an internal control framework

116. The management body is 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. Institutions should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures that should be approved by the management body.

117. Institutions should ensure that there is 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 (such as risk management, compliance and internal audit functions).

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

119. The internal control functions should verify that these policies, mechanisms and procedures are correctly implemented.

120. 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 on findings and corrective measures taken should be put in place.

12.2 Heads of internal control functions

121. A member of the management body in its management function may be responsible for an internal control function as referred to in section 15 provided that the member does not have other mandates which would compromise the members' internal control activities and the independence of the internal control function. Notwithstanding the overall responsibility of the management body for the institution, duties within the management body with respect to internal control functions should be assigned in a way that ensures the independence of the internal control functions.

122. When a head of an internal control function is not part of the management body in its management function, the respective position should be established at an adequate hierarchical level and be independent of the business areas it controls. To this end, the heads of the risk management and compliance functions should be directly accountable to

the management body, and the head of the internal audit function should be directly accountable to the management body in its supervisory function.

123. The head of an internal control function should be able to report directly to the management body in its supervisory function and raise concerns where specific developments affect or may affect the institution. This should not prevent the head of an internal control function to report directly to relevant committees or corporate bodies.

124. Institutions should have documented processes in place to assign the position of the head of an internal control function and to withdraw 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 prior approval of the management body in its supervisory function. For significant institutions, competent authorities should be promptly informed about the reasons of the appointment and the removal of a head of an internal control function.

12.3 Independence of internal control functions

125. In order for the internal control functions to be regarded as independent the following conditions should be met:

a. their staff does 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 responsibility of members of the management body for the institution, the head of an internal control function is not 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[21].

12.4 Combination of internal control functions

126. Taking into account the proportionality criteria listed in Title III, the risk management function and compliance function may be combined. The internal audit function should not be combined with another internal control function.

[21] See also guidelines on sound remuneration policies available under: https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies

12.5 Internal control functions, group context and outsourcing of internal control functions' tasks

127. The internal control framework of the institution concerned should be adapted at a solo basis to the specificity of its business, its complexity and the associated risks, taking also into account the group context. The institutions concerned have to organise the exchange of the information necessary to ensure that each management body, business line, internal units including internal control functions 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; - the head of the control functions at the group level and the management body of the institution.

128. The operational tasks of the internal control functions may be outsourced taking into account the proportionality criteria listed in Title III, 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.

12.6 Resources of internal control functions

129. Internal control functions should have sufficient resources and access to necessary training to fulfil their mission. They should have an adequate number of qualified staff (both at parent level and subsidiary level). Staff should be qualified on an on- going basis, and should receive training as necessary. Institutions 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 in particular the ones that can potentially generate material risks for the institution as well as to relevant risk-bearing subsidiaries.

13 Risk management framework

130. As part of the overall internal control framework, institutions should have a holistic institution wide risk management framework extending across all its business lines, internal units including internal control functions, recognising fully the economic substance of all its risk exposures. 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. 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, information technology, reputational, legal, conduct, compliance and strategic risks.

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

132. The risk management framework should enable the institution to make informed decisions. Risks should be evaluated bottom up and top down, within and across business lines, using consistent terminology and compatible methodologies throughout the institution and group.

133. 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.

134. The risk management framework should be subject to independent internal review 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, increasing complexity of the institution's business, risk profile and operating structure, geographic expansion, mergers and acquisitions and the introduction of new products or business lines.

135. 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.

136. Forward-looking tools (such as scenario analysis and stress tests) should identify and assess potential and stressed risk exposures under a range of assumed adverse circumstances; backward-looking tools should assess the actual risk profile and compare it against the institution's risk appetite and provide input for any adjustment required. Institutions should make appropriately conservative scenario and stressed assumptions.

137. Institutions should consider 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 superior strategy or execution by the institution.

138. The ultimate responsibility for risk assessment lies solely with the institution which accordingly should evaluate its risks critically and should not exclusively rely 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.

139. External risk assessments (including external credit ratings or externally purchased risk models) can help provide a more comprehensive estimate of risk. Institutions should be fully aware of the exact scope of such assessments.

140. Decisions which determine the level of risks taken should not only be based on quantitative information or model outputs, but should also take into account the practical and conceptual limitations of metrics and models, using a qualitative approach (including expert judgment and critical analysis). Relevant macroeconomic environment trends and data should be explicitly addressed to identify their potential impact on exposures and portfolios. Such assessments should be integrated into material risk decisions.

141. 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 and monitoring of risks. The reporting framework should be well defined, documented and duly approved by the management body.

142. 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.

14 New products and significant changes[22]

143. An institution should have in place a well-documented new product approval policy (NPAP) which addresses the development of new markets, products and services and significant changes to existing ones. The institution should also have appropriate change policies for material changes to processes (e.g. new outsourcing arrangements) and systems (e.g. IT change processes). The management body should approve this policy and endorse subsequent reviews of the policy and consider if approved products and changes require changes within the risk strategy, risk appetite and corresponding limits.

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

144. The compliance function, in collaboration with the risk management function, should be responsible for ensuring internal compliance with these policies. They should, on a periodical basis, check that the policies remain appropriate and propose amendments to the management body as appropriate.

145. An institution should have specific procedures for assessing compliance with these policies taking into account input from the risk management function. This should include a systematic prior assessment and approval by the compliance function, including a written opinion from the head of compliance or a person duly authorised by the head of compliance for new products or significant changes to existing products.

146. 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 definition of "new product/market/business/significant changes" to be used in the organisation and the internal functions to be involved in the decision-making process.

147. The NPAP should set out the main issues to be addressed before a decision is made. These should include regulatory compliance, accounting, pricing models, impacts on risk profile, capital adequacy and profitability, availability of adequate front, back and middle office resources and 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.

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

15 Internal control functions

15.1 Risk Management function (RMF)

149. Institutions should establish a comprehensive risk management function (RMF). The RMF should have sufficient authority, stature, resources taking into account the proportionality criteria listed in Title III to implement risk policies and the risk management framework as described in section 13.

150. The RMF should have direct access to the management body in its supervisory function and committees, where established, including in particular the risk committee, and to all business lines and other internal units that have the potential to generate risk as well as to relevant subsidiaries and affiliates.

151. Staff within RMF should possess sufficient knowledge, skills and experience on risk management techniques and procedures and on markets and products and have access to regular training.

152. The RMF should be independent of the business lines and units whose risks it controls but should not be prevented from interact with them. Interaction between the operational functions and the RMF should facilitate the objective that all the institution's staff bears responsibility for managing risk.

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

154. 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 of a group, to deliver an institution and group wide holistic view on all risks and that ensures that the risk strategy is complied with.

155. The RMF should provide relevant independent information, analyses and expert judgment on risk exposures, and advice on proposals and risk decisions made by business lines or internal units and 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.

15.1.1 RMF's role in risk strategy and decisions

156. 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 test 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 strategy of business units, including targets proposed by the business units, and should be involved before a decision is made by the management body in its management function concerning the risk strategies. Targets should be plausible and consistent.

157. The RMF's involvement in the 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.

15.1.2 RMF's role in material changes

158. In line with section 14, 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 on the change is taken.

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

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

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

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

162. The RMF should ensure that identification and assessment should not only be based on quantitative information or model outputs, but should also take into account the practical limitations of metrics and models, using a qualitative approach (including expert judgment and critical analysis). The RMF should keep the management body apprised of the assumptions used in and potential shortcomings of the risk models and analysis.

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

164. The RMF should ensure all identified risks can be effectively monitored by the business units. 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.

165. 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.

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

15.1.4 RMF's role in unapproved exposures

167. The RMF should be adequately involved in any changes to the institution's risk strategy, approved risk appetite and limits.

168. The RMF should independently assess breaches of risk appetite or limits (including the cause and 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 in its management function 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.

169. 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 .

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

15.1.5 Head of Risk Management Function

171. The head of the risk management function should be responsible for providing comprehensive and understandable information on risks, enabling the management body to understand the institution's overall risk profile. The same applies to the head of the risk management function of a parent institution regarding the group.

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

173. The head of risk management should be able to challenge decisions taken by the management body and the grounds for objections should be formally documented. If an institution wishes to grant the head of risk management 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 is involved.

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

15.2 Compliance function

175. An institution should establish a permanent and effective compliance function to manage its compliance risk and appoint a person responsible for this function across the entire institution (the Compliance Officer or Head of Compliance). The head of the compliance function should be able to report directly where appropriate and on his or her own initiative the management body in its supervisory function.

176. The compliance function should be independent of the business lines and internal units it controls and have sufficiently authority, stature and resources. Taking into account the proportionality criteria listed in Title III, this function may be assisted by the RMF or combined with the RMF or the legal division.

177. Staff within the compliance function should possess sufficient knowledge, skills and experience on compliance and procedures and have access to regular training.

178. 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 system to regularly follow changes on the law and regulation applicable to its activities.

179. The compliance function should advise the management body on laws, rules, regulations and standards the institutions need to comply with and assess the possible impact of any changes in the legal or regulatory environment on the institution's activities.

180. The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and the compliance policy is observed and report to the management body and communicate as appropriate with the RMF on the institution's management of compliance risk. The Compliance function and the RMF should cooperate and exchange information to perform their respective tasks. The findings of the compliance function should be taken into account by the management body and the RMF within the decision-making process.

181. In line with section 14 of these guidelines, the compliance function should also verify, in close cooperation with the RMF, that new products and new procedures comply with the current legal framework and, where appropriate, any known forthcoming changes to legislation, regulations and supervisory requirements.

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

15.3 Internal Audit function

183. An institution should set up an independent and effective internal audit function (IAF) taking into account the proportionality criteria listed in Title III and appoint a person responsible for this function across the entire institution. The IAF should be independent and have sufficiently authority, stature and resources. In particular, the institution should ensure that qualification of the IAF and its resources, in particular the monitoring tools and risk analysis methods are in adequacy with its size, locations and the nature, scale and complexity of the risks associated with the institution's model and business activities and risk culture and risk appetite.

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

185. The IAF should independently review the compliance of all activities and units of an institution including outsourced activities with institutions' policies and procedures and that should ensure that each entity within the group fall within the scope of the IAF.

186. The IAF should not be involved in designing, selecting, establishing and implementing specific internal control policies, mechanism 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.

187. The IAF should assess whether the quality of the institution's internal control framework as described in section 12 is both effective and efficient. In particular, the IAF should assess:

a. the appropriateness of the institutions' 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, 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…); and

e. the adequacy, quality and effectiveness of the controls performed and reporting by the first and the second lines of defense.

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

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

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

191. Internal audit work should be performed in accordance with an audit plan and detailed audit programs following a risk based approach. .

192. A audit plan should be drawn up at least once a year on the basis of the annual control objectives in line with the guidance of the management body in its supervisory function's..

193. All audit recommendations should be subject to a formal follow-up procedure by the respective levels of management to ensure and report their effective and timely resolution. The head of the IAF should be able to report directly where appropriate and on his own initiative the management body in its supervisory function of the non-implementation of the corrective measures decided on. This should not prevent him to report where relevant, to the risk committee.

16 Business continuity management

194. Institutions should establish a sound Business Continuity Management to ensure its ability to operate on an on-going basis and limit losses in the event of severe business disruption.

195. 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 to reduce the probability of such incidents or to transfer their financial impact (e.g. through insurance) to third parties.

196. In order to establish a sound business continuity management, 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. In addition, a specific independent Business Continuity function part of the RMF, the Operational Risk Management Function, should be actively involved for AMA institutions (i.e. institutions permitted to use Advanced Measurement Approaches (AMA) for operational risk in accordance with Article 312 of Regulation (EU) No 575/2013)[23]. The results of the analysis should contribute to define the institution's recovery priorities and objectives.

197. On the basis of the above analysis, an institution should put in place:

a. Contingency and business continuity plans to ensure an 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 it 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.

198. Contingency, business continuity and recovery plans should be documented and carefully implemented. The documentation should be available within the business lines, internal units and the RMF, and 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.

Q6: Are the guidelines in Title IV regarding the internal control framework appropriate and sufficiently clear?

Title V - Transparency

[23] See also draft Regulatory Technical Standards on assessment methodologies for the use of AMAs for operational risk: https://www.eba.europa.eu/regulation-and-policy/operational-risk/regulatory-technical-standards-on-assessment-methodologies-for-the-use-of-amas-for-operational-risk

199. 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.

200. 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.

201. Where parent undertakings are required by competent authorities under Article 106(2) Directive 2013/36/EU to publish annually a description of their legal structure and governance and organisational structure of the group of institutions, the information should include all entities within its group structure as defined within Directive 2013/34/EU[24], by country.

202. The publication should include at least:

a. an overview of the internal organisation of the institution and its group structure as defined within Directive 2013/34/EU and changes thereof, including the main reporting lines and responsibilities;

b. any material changes compared to the previous publication and respective date thereof;

c. new legal, governance or organisational structures;

d. an overview of material outsourcing of activities, processes and systems;

e. the nature, extent, purpose of close links as defined within point 38 of Article 4 of Regulation (EU) 575/2013between other credit institutions and other natural or legal persons, including the names and seat;

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

g. the key responsibilities of the management body;

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

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

i. an overview of the conflicts of interest policy applicable to the institutions and to the management body; and

j. an overview of the internal control framework including overview on the business continuity management framework.

Q7: Are the guidelines in Title V regarding transparency of the organization of the institution appropriate and sufficiently clear?

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

In line with Title II institutions should consider the following aspects when developing and documenting the written internal governance policy:

1. Shareholder structure
2. Group structure if applicable (legal and functional structure)
3. Composition and functioning of the management body (with impact on the group, if applicable)
   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 organization chart (with impact on the group, if applicable)
   a) Specialized committees
      i. composition
      ii. functioning
   b) management committee, if any
      i. composition
      ii. functioning (internal regulation)
5. Key functions holders
   a) Head of risk management function
   b) Head of compliance function
   c) Head of internal audit function
   d) Chief Financial Officer (CFO)
   e) other key function holders
6. Internal control framework
   a) description of each function including its organisation resources, stature , authority
   b) description of the risk management framework including risk strategy

c) weaknesses identified by each internal control functions and measures taken to address them

d) recommendations made by the internal audit function and measures taken to implement them

7. Organisational structure (with group impact, 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, ...

h) use of off-shore centres

8. Code of conduct and behaviour (with group impact, if applicable)

a) strategic objectives and company values

b) internal codes and regulations, prevention policy

c) conflicts of interest policy

d) whistleblowing

10. Status of the internal governance policy with date

a) development

b) last amendment

c) last assessment

d) approval by the management body

Accompanying documents

Draft cost-benefit analysis / impact assessment

1. Article 16(2) of the 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 financial system they collectively 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.

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 is updating the previously issued EBA guidelines on internal governance. The underlying reasons are mainly additions made in the CRD to the existing regulatory

framework. The GL were also restructured to increase their clarity and consistency with other work issued by the EBA in the meantime, in particular regarding the reinforcement of the requirements regarding risk oversight by management body and risk management function, 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 level of the group, parent undertakings and subsidiaries, including the branches and subsidiaries established in third countries and subsidiaries to which the CRD 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 enhance harmonisation of supervisory practices.

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

11. The EBA is updating the aforementioned GL on internal governance in line with the mandate given under Article 74 of the CRD and based on the reinforcement of the 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 should specify:

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

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

c. how the principle of proportionality is applied for both CA and institution; 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 and the EBA's Guidelines on internal governance published in 2011 and Guidelines on procedures and methodologies of the Supervisory Review and Evaluation Process (SREP), guidelines on sound remuneration policies and Guidelines on the assessment of the suitability of members of the management body and key function holders.

14. The IA covers Guidelines developed to ensure a harmonised application of additional governance requirements introduced by Directive 2013/36/EU and areas where the policy has changed. Areas which have not changed in substance and the underlying changes of the CRD and CRR have not been assessed.

15. The IA considers in particular the relevant GL for the following areas:

a. the involvement of the management body in the risk management and oversight;

b. the criteria for the application of the proportionality principle;

c. the organisation of internal control functions and in particular the risk management function.

D. Options considered

16. The following sets of policy options have been considered.

Option 1: Scope of Guidelines:

A) Providing guidelines on all aspects of internal governance arrangement including suitability of members of the management body, remuneration and disclosures.

B) Providing guidelines only on the aspects that have not been dealt with in other EBA products.

17. Option A appears to be more efficient for the addressees as all Guidelines regarding this particular area would be accessible in one single document. The costs for implementing of a one single set of Guidelines compared to separate sets of guidelines are the same.

18. Option B would allow for a stronger differentiation between Guidelines on internal governance arrangements, sound remuneration policies and suitability. Regarding the legal mandates provided to EBA, Option B would reflect better the CRD mandates provided. In any case all EBA Guidelines can be accessed via the EBA single rulebook.

19. Option B has been retained.

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

20. Option A: No further guidelines as the previous Guidelines were deemed sufficiently developed.

21. Option B: Reinforcement of the involvement of the management body regarding risk oversight by strengthening its duties and responsibilities distinguishing between the management body in its supervisory and the management function. In particular the management body in its supervisory function should monitor that the strategic objectives, the organizational structure, 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 functions 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.

22. Option A is not recommended as it would not lead to a further degree of harmonisation and would not improve sound risk management practices and involvement of the management body in risk oversight and more generally in internal governance arrangements.

23. Option B would increase risk oversight by the management and risk culture within institutions in line with international standards. While some additional guidelines were provided regarding in responsibilities for the management body, it is not expected that this increases the costs of the governance arrangements already implemented within institutions and for supervision by CA. The only costs will be triggered by assessing and raising the qualification and the available resources of members of management body particularly regarding risk management. This will also depend on the size and complexity of institutions.

24. Option B was retained.

Option 3: Proportionality

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

26. Option A: Retaining the neutral approach taken under the EBA GL.

27. Option B: providing a set of criteria in line with Article 74 (2) of the CRD for the application of proportionality in a harmonised way.

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

29. Option B provides a non-limitative list of criteria to take into account to apply the principle of proportionality. All institutions and CA should take into account at least those criteria which will ensure consistency for the application of the proportionality. No additional cost are raised by additional guidelines for both CA and institutions.

30. Option B was retained

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

31. Option A: No further guidelines as the previous Guidelines were deemed sufficiently developed.

32. Option B: Strengthening the guidelines regarding resources, authority and stature only for the risk management function.

33. Option C: Strengthening the guidelines regarding resources, authority and stature, of all internal control function.

34. Option A is not recommended as it would not lead to a further degree of harmonisation and would not improve sound risk management practices and involvement of the management body in risk oversight and more generally in internal governance arrangements.

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

36. Option C provides for consistencies between the internal control functions. While one might argue that this would cause additional cost, those costs are only needed to establish a sound internal control framework to ensure independence to internal control function. This was already required by existing regulation. However, stronger internal functions within institutions may be more costly in terms of staff costs or reorganisation, but institutions will also benefit from improved framework, which will lead to a better alignment of the risk profile with the risk appetite as set by the management body.

37. Option C was retained

E. Cost-Benefit Analysis

38. Overall the guidelines, compared to the baseline scenario, would create very low additional recurring costs for institutions, mainly driven by reorganising their internal control framework. In addition, the minor increase of costs would be compensated through 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.

39. The implementation of the Guidelines by competent authorities will trigger low one off costs for changing existing rule-/methodologies/manuals and to inform staff members and the sector regarding those changes. As the changes are limited and are mainly an update of existing guidelines the costs should be relatively low.

40. Furthermore, the Guidelines are in line with international internal governance standards, therefore no impact on the level playing field compared to non EU –institutions are expected.

Q8: Are the findings and conclusions of the impact assessments appropriate; please provide to the extent possible an estimate of the cost to implement the Guidelines differentiating of one-off and ongoing costs?

Overview of questions for consultation

Q1: Are the guidelines regarding the subject matter, scope, definitions and implementation appropriate and sufficiently clear?

Q2: Are there any conflicts between the responsibilities assigned by national company law to a specific function of the management body and the responsibilities assigned by the Guidelines, in particular within paragraph 23, to either the management or supervisory function?

Q3: Are the guidelines in Title I regarding the role of the management body appropriate and sufficiently clear?

Q4: Are the guidelines in Title II regarding the internal governance policy, risk culture and business conduct appropriate and sufficiently clear?

Q5: Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear?

Q6: Are the guidelines in Title IV regarding the internal control framework appropriate and sufficiently clear?

Q7: Are the guidelines in Title V regarding transparency of the organization of the institution appropriate and sufficiently clear?

Q8: Are the findings and conclusions of the impact assessments appropriate; please provide to the extent possible an estimate of the cost to implement the Guidelines differentiating of one-off and ongoing costs?