NautaDutilh

EBA GUIDELINES ON INTERNAL GOVERNANCE

Comparison 2017 and 2011 version

Amsterdam
15 June 2018

EXECUTIVE SUMMARY

- **Attention for different management body structures**

  - The Guidelines use the terms 'management body', 'management body in its management function' and 'management body in its supervisory function'. The 'management body' should be understood as having both management (executive) and supervisory (non-executive) functions. In the Netherlands, we would refer to the Executive Board (*Raad van Bestuur*) and the Supervisory Board (*Raad van Commissarissen*). In the event the Guidelines refer to the management board in both functions, we will refer to both boards.

  - The members of the Executive Committee are understood as constituting the members of the Executive Board.

- **Group-wide compliance with Guidelines**

  - Parent undertakings and subsidiaries subject to CRD IV should ensure group-wide compliance with the Guidelines; must implement governance arrangements and processes in their subsidiaries that are not subject to CRD IV.

- **Know your board structure**

  - All members of both the Executive Board and the Supervisory Board should be fully aware of the structure and responsibilities of these Boards, and of the division of tasks between different functions of these Boards and its committees.

- **Emphasis on the role of the chair of the management body**

  - The chair of the management body is put forward as a leader; has an obligation to contribute to the efficient flow of information within the Executive and Supervisory Board and between both Boards and the committees thereof; the chair is responsible for its effective overall functioning of both Boards.

- **Obligatory establishment of Committees for significant institutions**

  - All institutions that are themselves significant, must establish risk, nomination and remuneration committees to advise the Supervisory Board and to prepare the decisions to be taken by this Board.
  - Institutions should ensure a clear allocation and distribution of duties and tasks between specialised committees of the Supervisory Board.

- Committees should document the agendas of committee meetings and their main results and conclusions.
- Non-significant institutions may combine committees, but must document the reasons why and how the approach achieves the objectives of the committees.
-

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

- Both the Executive and the Supervisory Board must understand the set-up complex structures, their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. These complex and potentially non-transparent structures should be approved and maintained only when their purpose has been clearly defined and understood, all materials risks have been identified and can be managed and that effective oversight is ensured.
- Institutions should take the same risk management measures as for the institution's own business activities when they perform non-standard or on-transparent activities for clients that pose similar internal governance challenges and create significant operational and reputational risks.

- **Risk Culture and Business Conduct**

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

- **Amendments to existing guidelines regarding New Product Approval Policy (NPAP)**

- The NPAP should encompass material changes to related processes, such as outsourcing arrangements, and (IT-)systems; the NPAP should also ensure that approved products and changes are consistent with the risk strategy and risk appetite of the institution and the corresponding limits.
- Both the risk management function and compliance function should be involved in approving new products or significant changes to existing products, processes and systems.

- **Prior approval of Supervisory Board necessary for removal of heads of internal control functions**

- Under the new Guidelines, the heads of internal control functions, i.e. the risk management function, the internal audit function and the compliance function, should in any case not be removed without the prior approval of the management body in its supervisory function. Currently, only the removal of the head of the risk management function requires prior approval of the Supervisory Board (Article 76(5) of CRD IV).

EBA Guidelines 2017	EBA Guidelines 2011	Differences
GUIDELINES		
1. Compliance and reporting obligations		Status of the guidelines and reporting requirements are part of the new Guidelines. Under the old Guidelines, these paragraphs were only part of the introduction to the Guidelines.
Status of these guidelines	***Status of the guidelines***	
1. These guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010. 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.	1. This document contains guidelines issued under Article 16 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (EBA Regulation). In accordance with Article 16(3) of the EBA Regulation, competent authorities and financial market participants must make every effort to comply with the guidelines.	No differences.
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	2. Guidelines set out EBA‟s view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. EBA therefore expects all competent authorities and financial market participants to whom guidelines apply to comply with guidelines unless otherwise stated. Competent authorities to whom guidelines apply should comply by incorporating them into their supervisory practices (e.g. by amending their legal framework or their supervisory rules and/or guidance or supervisory processes), including where particular guidelines within the	No differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	document are directed primarily at institutions.	
Reporting requirements	***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 21.05.2018. In the absence of any notification by this deadline, competent authority will be considered by the EBA to be noncompliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2017/11'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authority. Any change in the status of compliance must also be reported to EBA.	3. Competent authorities must notify EBA whether they comply or intend to comply with these guidelines, or with reasons for non-compliance, by 28 November 2011. Notifications should be sent by persons authorised to notify EBA on behalf of competent authorities to compliance@eba.europa.eu.	Pursuant to the new Guidelines, the competent authority will be considered to be noncompliant in the event this authority fails to notify before a given deadline. Furthermore, any change in the status of compliance must also be reported by the competent authority to EBA.
4. Notifications will be published on the EBA website, in line with Article 16(3) of Regulation (EU) No 1093/2010.	4. The notification of competent authorities mentioned in the previous paragraph shall be published on the EBA website, as per article 16 of EBA Regulation.	No differences.
2. Subject matter, scope and definitions	**Title I -Subject matter, Scope and definitions**	
Subject matter	***1. Subject matter***	
5. These guidelines specify the internal governance arrangements, processes and mechanisms that credit institutions and investment firms must implement in accordance with Article 74(1) of Directive 2013/36/EU to ensure effective and prudent management of the institution.	The Guidelines aim to harmonise supervisory expectations and to improve the sound implementation of internal governance arrangements in line with Article 22 and Annex V of Directive 2006/48/EC and national company laws.	
Addressees		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
6. These guidelines are addressed to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013, including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013, and to institutions as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013.		The new Guidelines explicitly refer to groups of addressees: (i) the competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013, including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013; and (ii) credit institutions and investment firms as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013.
Scope of application	**2. Scope and level of application**	
7. These guidelines apply in relation to institutions' governance arrangements, including their organisational structure and the corresponding lines of responsibility, processes to identify, manage, monitor and report the risks they are or might be exposed to, and internal control framework	1.Competent authorities shall require institutions to comply with the provisions laid down in these Guidelines on Internal Governance. 2. The application of these Guidelines shall be reviewed by competent authorities as part of their Supervisory Review and Evaluation Process. 3. The Guidelines apply to institutions on a solo basis and to parent undertakings and subsidiaries on a consolidated or sub-consolidated basis, unless stated otherwise.	
8. The guidelines intend to embrace all existing board structures and do not advocate any particular structure. The guidelines do not interfere with the general allocation of competences in accordance with national company law. Accordingly, they should be applied irrespective of the board structure used (unitary and/or a dual board structure and/or another structure) across Member States. The		In the new Guidelines, it is made explicit that these Guidelines intend to embrace all existing board structures and do not advocate any particular structure. Under the new Guidelines, the management body should be understood as having management (executive) and supervisory (non-executive) functions.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
management body, as defined in points (7) and (8) of Article 3(1) of Directive 2013/36/EU, should be understood as having management (executive) and supervisory (non-executive) functions.		
9. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (nonexecutive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law. When implementing these guidelines, competent authorities should take into account their national company law and specify, where necessary, to which body or members of the management body those functions should apply.		Competent authorities should, when implementing these guidelines, take into account their national company law and specify, where necessary, to which body or members of the management body those functions should apply.
10. In Member States where the management body delegates, partially or fully, the executive functions to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons who perform those executive functions on the basis of that delegation should be understood as constituting the management function of the management body. For the purposes of these guidelines, any reference to the management body in its management function should be understood as including also		An important difference is the attention for the position of the Executive Committee within the company: the executive functions to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons who perform those executive functions on the basis of that delegation should be understood as constituting the management function of the management body (…) even if they have not been proposed or appointed as formal members of the institution's governing body or bodies under national law.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
the members of the executive body or the CEO, as defined in these guidelines, even if they have not been proposed or appointed as formal members of the institution's governing body or bodies under national law.		
11. In Member States where some responsibilities are directly exercised by shareholders, members or owners of the institution instead of the management body, institutions should ensure that such responsibilities and related decisions are in line, as far as possible, with the guidelines applicable to the management body.		
12. The definitions of CEO, chief financial officer (CFO) and key function holder used in these guidelines are purely functional and are not intended to impose the appointment of those officers or the creation of such positions unless prescribed by relevant EU or national law.		
13. Institutions should comply and competent authorities should ensure that institutions comply with these guidelines on an individual, sub consolidated and consolidated basis, in accordance with the level of application set out in Article 109 of Directive 2013/36/EU.	3. The Guidelines apply to institutions on a solo basis and to parent undertakings and subsidiaries on a consolidated or sub-consolidated basis, unless stated otherwise.	A difference is that institutions under the new Guidelines should ensure group-wide compliance with the Guidelines in accordance with the level of application set out in Article 109 CRD IV - "In particular, they shall ensure that parent undertakings and subsidiaries subject to this Directive implement such arrangements, processes and mechanisms in their subsidiaries not subject to this Directive."
Definitions	***3. Definitions***	
14. Unless otherwise specified, terms used and defined in Directive 2013/36/EU have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following	1. In these guidelines the term management body shall have the following meaning: the governing body (or bodies) of an institution, comprising the supervisory and the managerial	The new Guidelines entail a more comprehensive array of definitions. In the new Guidelines, (i) risk appetite; (ii) risk capacity; (iii) risk culture; (iv) staff; (v) Chief Executive Officer; (vi) Chief financial officer (CFO);

EBA Guidelines 2017	EBA Guidelines 2011	Differences
definitions apply: **Risk appetite** means the aggregate level and types of risk an institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives. **Risk capacity** means the maximum level of risk an institution is able to assume given its capital base, its risk management and control capabilities, and its regulatory constraints. **Risk culture** means an institution's norms, attitudes and behaviours related to risk awareness, risk- taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day **Institutions** means credit institutions and investment firms as defined in Article 4(1)(1) and (2), respectively, of Regulation (EU) No 575/2013. **Staff** means all employees of an institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to Directive 2013/36/EU, and all members of the management body in its management function and in its supervisory function.	function, which has the ultimate decision-making authority and is empowered to set the institution's strategy, objectives and overall direction. The management body shall include persons who effectively direct the business of an institution. 2. In these guidelines the term institutions shall have the following meaning: credit institutions and investment firms according to Directives 2006/48/EC and 2006/49/EC.	(vii) Heads of internal control functions; (viii) Key function holders; (ix) Prudential consolidation; (x) Consolidating institution; (xi) Significant institutions; (xii) Listed CRD-institution; (xiii) Shareholder; and (xiv) Directorship.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
Chief executive officer (CEO) means the person who is responsible for managing and steering the overall business activities of an institution. **Chief financial officer (CFO)** means the person who is overall responsible for managing all of the following activities: financial resources management, financial planning and financial reporting. **Heads of internal control functions** means the persons at the highest hierarchical level in charge of effectively managing the day-to day operation of the independent risk management, compliance and internal audit functions. **Key function holders** means persons who have significant influence over the direction of the institution but who are not members of the management body and are not the CEO. They include the heads of internal control functions and the CFO, where they are not members of the management body, and, where identified on a risk-based approach by institutions, other key function holders. Other key function holders might include heads of significant business lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions. **Prudential consolidation** means the application of the prudential rules set out in		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
Directive 2013/36/EU and Regulation (EU) No 575/2013 on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013. Prudential consolidation includes all subsidiaries that are institutions or financial institutions, as defined in Article 4(3) and (26), respectively, of Regulation (EU) No 575/2013, and may also include ancillary services undertakings, as defined in Article 2(18) of that Regulation, established in and outside the EU. **Consolidating institution** means an institution that is required to abide by the prudential requirements on the basis of the consolidated situation in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013. **Significant institutions** means institutions referred to in Article 131 of Directive 2013/36/EU (global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs)), and, as appropriate, other institutions determined by the competent authority or national law, based on an assessment of the institutions' size and internal organisation, and the nature, scope and complexity of their activities. **Listed CRD-institution** means institutions whose financial instruments are admitted to trading on a regulated market or on a multilateral trading facility as defined under		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
Article 4, paragraphs (21) and (22) of Directive 2014/65/EU, in one or more Member States. **Shareholder** means a person who owns shares in an institution or, depending on the legal form of an institution, other owners or members of the institution. **Directorship** means a position as a member of the management body of an institution or another legal entity.		
3. Implementation	**Title III – Final Provisions and Implementation**	
Date of application	**35. Date of application**	
15. These guidelines apply from 30 June 2018.	Competent authorities shall implement the Guidelines on Internal Governance by incorporating them within their supervisory procedures by 31 March 2012. After that date, competent authorities should ensure that institutions comply with it effectively.	
Repeal	**34. Repeal**	
16. The EBA guidelines on internal governance (GL 44) of 27 September 2011 are repealed with effect from 30 June 2018.	With the adoption and publication of these Internal Governance Guidelines, the following Guidelines are repealed: section 2.1 of the CEBS Guidelines on the Application of the Supervisory Review Process (dated 25 January 2006), entitled „Guidelines on Internal Governance"; the „High Level Principles for Remuneration Policies" (dated 20 April 2009) and the „High Level Principles for Risk Management" (dated 16 February 2010).	
4. Guidelines		
Title I – Proportionality	***2.4 Scope and level of application***	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
17. The proportionality principle encoded in Article 74(2) of Directive 2013/36/EU aims to ensure that internal governance arrangements are consistent with the individual risk profile and business model of the institution, so that the objectives of the regulatory requirements are effectively achieved.		The proportionality principle under the new Guidelines must be applied in a way that is consistent with the individual risk profile in addition to the business model of the institution.
18. Institutions should take into account their size and internal organisation, and the nature, scale and complexity of their activities, when developing and implementing internal governance arrangements. Significant institutions should have more sophisticated governance arrangements, while small and less complex institutions may implement simpler governance arrangements.	4. Proportionality, as laid down in Directives 2006/48 and 2006/49 (as amended), applies to all provisions contained in the Guidelines. An institution may demonstrate how its approach, reflecting the nature, scale and complexity of its activities, meets the outcome required by the Guidelines.	
19. For the purpose of the application of the principle of proportionality and in order to ensure an appropriate implementation of the requirements, the following criteria should be taken into account by institutions and competent authorities: a. the size in terms of the balance-sheet total of the institution and its subsidiaries within the scope of prudential consolidation; b. the geographical presence of the institution and the size of its operations in each jurisdiction; c. the legal form of the institution, including whether the institution is part of a group and, if so, the proportionality assessment for the group;		The new Guidelines specify the criteria that should be taken into account by institutions and competent authorities with regard to the application of the principle of proportionality.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
d. whether the institution is listed or not; e. whether the institution is authorised to use internal models for the measurement of capital requirements (e.g. the Internal Ratings Based Approach); f. the type of authorised activities and services performed by the institution (e.g. see also Annex 1 to Directive 2013/36/EU and Annex 1 to Directive 2014/65/EU); g. the underlying business model and strategy; the nature and complexity of the business activities, and the institution's organisational structure; h. the risk strategy, risk appetite and actual risk profile of the institution, taking into account also the result of the SREP capital and SREP liquidity assessments; i. the ownership and funding structure of the institution; j. the type of clients (e.g. retail, corporate, institutional, small businesses, public entities) and the complexity of the products or contracts; k. the outsourced activities and distribution channels; and l. the existing information technology (IT) systems, including continuity systems and outsourcing activities in this area.		
Title II – Role and composition of the management body and committees	***B. Management body - B.1 Duties and responsibilities of the management body***	
1 Role and responsibilities of the management body	*8. Responsibilities of the management body*	
20. In accordance with Article 88(1) of	1. The management body shall have the overall	Under the new Guidelines, the management body must

EBA Guidelines 2017	EBA Guidelines 2011	Differences
Directive 2013/36/EU, the management body must have ultimate and overall responsibility for the institution and defines, oversees and is accountable for the implementation of the governance arrangements within the institution that ensure effective and prudent management of the institution.	responsibility for the institution and shall set the institution's strategy. (…)	*define*, *oversee* and *is accountable for* the implementation of the governance arrangements within the institution. In a two-tier model this means that the Executive Board should define the implementation of the governance arrangements within the institution, whereas the Supervisory Board should oversee this implementation.
21. The duties of the management body should be clearly defined, distinguishing between the duties of the management (executive) function and of the supervisory (non-executive) function. The responsibilities and duties of the management body should be described in a written document and duly approved by the management body.	1. (…) The responsibilities of the management body shall be clearly defined in a written document and approved.	Under the new Guidelines, a distinction is made between the duties and responsibilities of the management (executive) function and the supervisory (non-executive) function of the management body.
22. All members of the management body should be fully aware of the structure and responsibilities of the management body, and of the division of tasks between different functions of the management body and its committees. In order to have appropriate checks and balances in place, its decision-making should not be dominated by a single member or a small subset of its members. The management body in its supervisory function and in its management function should interact effectively. Both functions should provide each other with sufficient information to allow them to perform their respective roles.		Under the new Guidelines, all members of both Boards should be fully aware of the structure and responsibilities of the management body, and of the division of tasks between different functions of the management body and its committees (*Know your management body structure*). In the consultation phase of the Guidelines, EBA was asked how to make sure that the decision-making within the management body could not be dominated by a single member or a small subset of members. The EBA has not answered this question and reiterated that the management body should ensure that its decision making cannot be dominated by a single member or a small subset of members.
23. The management body's responsibilities should include setting, approving and overseeing the implementation of:	2. The key responsibilities of the management body should include setting and overseeing: a. the overall business strategy of the institution	This new Guideline defines 13 (the Old Guideline distinguishes 8) main tasks of the management body. With regard to these main tasks, the management body does not only have the responsibility to set the

EBA Guidelines 2017	EBA Guidelines 2011	Differences
a. the overall business strategy and the key policies of the institution within the applicable legal and regulatory framework, taking into account the institution's long-term financial interests and solvency; b. the overall risk strategy, including the institution's risk appetite and its risk management framework and measures to ensure that the management body devotes sufficient time to risk issues; c. an adequate and effective internal governance and internal control framework that includes a clear organisational structure and well-functioning independent internal risk management, compliance and audit functions that have sufficient authority, stature and resources to perform their functions; d. the amounts, types and distribution of both internal capital and regulatory capital to adequately cover the risks of the institution; e. targets for the liquidity management of the institution; f. a remuneration policy that is in line with the remuneration principles set out in Articles 92 to 95 of Directive 2013/36/EU and the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU; g. arrangements aimed at ensuring that the individual and collective suitability assessments of the management body are carried out effectively, that the composition and succession planning of the management	within the applicable legal and regulatory framework taking into account the institution's long-term financial interests and solvency; b. the overall risk strategy and policy of the institution, including its risk tolerance/appetite and its risk management framework; c. the amounts, types and distribution of both internal capital and own funds adequate to cover the risks of the institution; d. a robust and transparent organisational structure with effective communication and reporting channels; e. a policy on the nomination and succession of individuals with key functions in the institution; f. a remuneration framework that is in line with the risk strategies of the institution; g. the governance principles and corporate values of the institution, including through a code of conduct or comparable document; and h. an adequate and effective internal control framework, that includes well-functioning Risk Control, Compliance and Internal Audit functions as well as an appropriate financial reporting and accounting framework.	policies/strategy and to oversee the implementation thereof, but there is also a responsibility to *approve*. This raises the question if under Dutch law, the Supervisory Board has a right of approval with regard to these 13 main tasks. In a two-tier model, the allocation of the tasks would be that the Executive Board would include the setting of the strategy and the other mentioned subjects, whereas the Supervisory Board would oversee the implementation thereof.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
body are appropriate, and that the management body performs its functions effectively; h. a selection and suitability assessment process for key function holders; i. arrangements aimed at ensuring the internal functioning of each committee of the management body, when established, detailing the: i. role, composition and tasks of each of them; ii. appropriate information flow, including the documentation of recommendations and conclusions, and reporting lines between each committee and the management body, competent authorities and other parties; j. a risk culture in line with Section 9 of these guidelines, which addresses the institution's risk awareness and risk-taking behaviour; k. a corporate culture and values in line with Section 10, which fosters responsible and ethical behaviour, including a code of conduct or similar instrument; l. a conflict of interest policy at institutional level in line with Section 11 and for staff in line with Section 12; and m. arrangements aimed at ensuring the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards.		
24. The management body must oversee the process of disclosure and communications with external stakeholders and competent authorities.	3. (…) The management body is responsible for appropriate communication with supervisory authorities and other interested parties.	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
25. All members of the management body should be informed about the overall activity, financial and risk situation of the institution, taking into account the economic environment, and about decisions taken that have a major impact on the institution's business.		
26. A member of the management body may be responsible for an internal control function as referred to in Title V, Section 19.1, provided that the member does not have other mandates that would compromise the member's internal control activities and the independence of the internal control function.		
27. The management body should monitor, periodically review and address any weaknesses identified regarding the implementation of processes, strategies and policies related to the responsibilities listed in paragraphs 23 and 24. The internal governance framework and its implementation should be reviewed and updated on a periodic basis taking into account the proportionality principle, as further explained in Title I. A deeper review should be carried out where material changes affect the institution.	3. The management body should also regularly review and adjust these policies and strategies. (…) 9. Assessment of the internal governance framework 1. The management body shall monitor and periodically assess the effectiveness of the institution's internal governance framework. 2. A review of the internal governance framework and its implementation should be performed at least annually. It should focus on any changes in internal and external factors affecting the institution.	
2 Management function of the management body	*10. Management and supervisory functions of the management body*	
28. The management body in its management function should engage actively in the business		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
of an institution and should take decisions on a sound and well informed basis.		
29. The management body in its management function should be responsible for the implementation of the strategies set by the management body and discuss regularly the implementation and appropriateness of those strategies with the management body in its supervisory function. The operational implementation may be performed by the institution's management.		Under the new Guidelines, the management body in its management function should be responsible for the implementation of the strategies set by the management body. Important difference with the allocation of authorities within the company under Dutch law is that this Guideline assumes that the strategies are set by the management body *in its entirety*, both the management (executive) function and the supervisory (non-executive) function of the management body. Under Dutch law, the Executive Board sets the strategy and the Supervisory Board oversees the implementation thereof.
30. The management body in its management function should constructively challenge and critically review propositions, explanations and information received when exercising its judgement and taking decisions. The management body in its management function should comprehensively report, and inform regularly and where necessary without undue delay the management body in its supervisory function of the relevant elements for the assessment of a situation, the risks and developments affecting or that may affect the institution, e.g. material decisions on business activities and risks taken, the evaluation of the institution's economic and business environment, liquidity and sound capital base,		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
and assessment of its material risk exposures.		
3 Supervisory function of the management body	10. Management and supervisory functions of the management body	
31. The role of the members of the management body in its supervisory function should include monitoring and constructively challenging the strategy of the institution.		The new Guidelines entail more detailed requirements regarding the Supervisory Board in particular the composition and function of the committees of the management body in its supervisory function. See hereafter.
32. Without prejudice to national law the management body in its supervisory function should include independent members as provided for in Section 9.3 of the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.		
33. Without prejudice to the responsibilities assigned under the applicable national company law, the management body in its supervisory function should: a. oversee and monitor management decision-making and actions and provide effective oversight of the management body in its management function, including monitoring and scrutinising its individual and collective performance and the implementation of the institution's strategy and objectives; b. constructively challenge and critically review proposals and information provided by members of the management body in its management function, as well as its decisions; c. taking into account the proportionality	2. The management body in its supervisory function should: a. be ready and able to challenge and review critically in a constructive manner propositions, explanations and information provided by members of the management body in its management function; b. monitor that the strategy, the risk tolerance/appetite and the policies of the institution are implemented consistently and performance standards are maintained in line with its long-term financial interests and solvency; and c. monitor the performance of the members of the management body in its management function against those standards.	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
principle as set out in Title I, appropriately fulfil the duties and role of the risk committee, the remuneration committee and the nomination committee, where no such committees have been set up; d. ensure and periodically assess the effectiveness of the institution's internal governance framework and take appropriate steps to address any identified deficiencies; e. oversee and monitor that the institution's strategic objectives, organisational structure and risk strategy, including its risk appetite and risk management framework, as well as other policies (e.g. remuneration policy) and the disclosure framework are implemented consistently; f. monitor that the risk culture of the institution is implemented consistently; g. oversee the implementation and maintenance of a code of conduct or similar and effective policies to identify, manage and mitigate actual and potential conflicts of interest; h. oversee the integrity of financial information and reporting, and the internal control framework, including an effective and sound risk management framework; i. ensure that the heads of internal control functions are able to act independently and, regardless the responsibility to report to other internal bodies, business lines or units, can raise concerns and warn the management body in its supervisory function directly, where necessary, when adverse risk developments	3. The management body in its management function should coordinate the institution's business and risk strategies with the management body in its supervisory function and discuss regularly the implementation of these strategies with the management body in its supervisory function.	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
affect or may affect the institution; and j. monitor the implementation of the internal audit plan, after the prior involvement of the risk and audit committees, where such committees are established.		
	11. Composition, appointment and succession of the management body	
	1. The management body shall have an adequate number of members and an appropriate composition. The management body shall have policies for selecting, monitoring and planning the succession of its members. 2. An institution should set the size and composition of its management body, taking into account the size and complexity of the institution and the nature and scope of its activities. The selection of members of the management body should ensure sufficient collective expertise. 3. The management body should identify and select qualified and experienced candidates and ensure appropriate succession planning for the management body, giving due consideration to any other legal requirements regarding composition, appointment or succession. 4. The management body should ensure that an institution has policies for selecting new members and re-appointing existing members. These policies should include the making of a	Specific guidelines regarding the composition, appointment and succession of the management body in its entirety are repealed in the Guidelines on internal governance. Guidelines on the composition of the management body and the appointment and succession of its members are laid down in the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU. See Guideline 129 and further.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	description of the necessary competencies and skills to ensure sufficient expertise. 5. Members of the management body should be appointed for an appropriate period. Nominations for re-appointment should be based on the profile referred to above and should only take place after careful consideration of the performance of the member during the last term. 6. When establishing a succession plan for its members, the management body should consider the expiry date of each member's contract or mandate to prevent, where possible, too many members having to be replaced simultaneously.	
	12. Commitment, independence and managing conflicts of interest in the management body	
	1. Members of the management body shall engage actively in the business of an institution and shall be able to make their own sound, objective and independent decisions and judgements. 2. The selection of members of the management body should ensure that there is sufficient expertise and independence within the management body. An institution should ensure that members of the management body are able to commit enough time and effort to fulfil their responsibilities effectively.	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	3. Members of the management body should only have a limited number of mandates or other professional high time consuming activities. Moreover, members should inform the institution of their secondary professional activities (e.g. mandates in other companies). Because the chair has more responsibilities and duties, a greater devotion of time should be expected from him/her. 4. A minimum expected time commitment for all members of the management body should be indicated in a written document. When considering the appointment of a new member, or being informed of a new mandate by an existing member, members of the management body should challenge how the individual will spend sufficient time fulfilling their responsibilities to the institution. Attendance of the members of the management body in its supervisory function should be disclosed. An institution should also consider disclosing the long-term absence of members of the management body in its management function. 5. The members of the management body should be able to act objective, critically and independently. Measure to enhance the ability to exercise objective and independent judgement should include, recruiting members from a sufficiently broad population of candidates and having a sufficient number of non-executive members.	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	6. The management body should have a written policy on managing conflicts of interests for its members. The policy should specify: a. a member's duty to avoid conflicts of interest that have not been disclosed to and approved by the management body, but otherwise to ensure conflicts are managed appropriately; b. a review or approval process for members to follow before they engage in certain activities (such as serving on another management body) to ensure such new engagement would not create a conflict of interest; c. a member's duty to inform the institution of any matter that may result, or has already resulted, in a conflict of interest; d. a member's responsibility to abstain from participating in the decision-making or voting on any matter where the member may have a conflict of interest or where the member's objectivity or ability to properly fulfil his/her duties to the institution may be otherwise compromised; e. adequate procedures for transactions with related parties to be made on an arms-length basis; and f. the way in which the management body would deal with any noncompliance with the policy.	
	13. Qualifications of the management body	
	1. Members of the management body shall be and remain qualified, including through training, for their positions. They shall have a	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	clear understanding of the institution's governance arrangements and their role in them. 2. The members of the management body, both individually and collectively, should have the necessary expertise, experience, competencies, understanding and personal qualities, including professionalism and personal integrity, to properly carry out their duties. 3. Members of the management body should have an up-to-date understanding of the business of the institution, at a level commensurate with their responsibilities. This includes appropriate understanding of those areas for which they are not directly responsible but are collectively accountable. 4. Collectively, they should have a full understanding of the nature of the business and its associated risks and have adequate expertise and experience relevant to each of the material activities the institution intends to pursue in order to enable effective governance and oversight. 5. An institution should have a sound process in place to ensure that the management body members, individually and collectively, have sufficient qualifications. 6. Members of the management body should acquire, maintain and deepen their knowledge	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	and skills to fulfil their responsibilities. Institutions should ensure that members have access to individually tailored training programmes which should take account of any gaps in the knowledge profile the institution needs and members' actual knowledge. Areas that might be covered include the institution's risk management tools and models, new developments, changes within the organisation, complex products, new products or markets and mergers. Training should also cover business areas individual members are not directly responsibility for. The management body should dedicate sufficient time, budget and other resources to training.	
4 Role of the chair of the management body	*14. Organisational functioning of the management body - Role of the chair of the management body*	
34. The chair of the management body should lead the management body, should contribute to an efficient flow of information within the management body and between the management body and the committees thereof, where established, and should be responsible for its effective overall functioning.	4. The chair should ensure that management body decisions are taken on a sound and well-informed basis. (…) He or she should encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.	An important difference here is that the chair of the management body is put forward as a leader of the management body and has an obligation to contribute to an efficient flow of information within the management body and between the management body and the committees thereof, where established, and should be responsible for its effective overall functioning. Under Dutch law, this regards the chairman of the Supervisory Board.
35. The chair should encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.	4. (…) He or she should encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.	
36. As a general principle, the chair of the	5. In a one tier system, the chair of the	Under the new Guidelines, the chair of the management

EBA Guidelines 2017	EBA Guidelines 2011	Differences
management body should be a non-executive member. Where the chair is permitted to assume executive duties, the institution should have measures in place to mitigate any adverse impact on the institution's checks and balances (e.g. by designating a lead board member or a senior independent board member, or by having a larger number of non-executive members within the management body in its supervisory function). In particular, in accordance with Article 88(1)(e) of Directive 2013/36/EU, the chair of the management body in its supervisory function of an institution must not exercise simultaneously the functions of a CEO within the same institution, unless justified by the institution and authorised by competent authorities.	management body and the chief executive officer of an institution should not be the same person. Where the chair of the management body is also the chief executive officer of the institution, the institution should have measures in place to minimise the potential detriment on its checks and balances.	body should, as a general principle, be a non-executive member. Under Dutch law, this regards the chairman of the Supervisory Board which does not perform an executive function.
37. The chair should set meeting agendas and ensure that strategic issues are discussed with priority. He or she should ensure that decisions of the management body are taken on a sound and well informed basis and that documents and information are received in enough time before the meeting.		
38. The chair of the management body should contribute to a clear allocation of duties between members of the management body and the existence of an efficient flow of information between them, in order to allow the members of the management body in its supervisory function to constructively contribute to discussions and to cast their votes on a sound and well-informed basis.		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
5 Committees of the management body in its supervisory function	*14. Organisational functioning of the management body*	
5.1 Setting up committees	*Specialised committees of the management body*	
39. In accordance with Article 109(1) of Directive 2013/36/EU in conjunction with Articles 76(3), 88(2), and 95(1) of Directive 2013/36/EU, all institutions that are themselves significant, considering the individual, sub-consolidated and consolidated levels, must establish risk, nomination and remuneration committees to advise the management body in its supervisory function and to prepare the decisions to be taken by this body. Non-significant institutions, including when they are within the scope of prudential consolidation of an institution that is significant in a sub-consolidated or consolidated situation, are not obliged to establish those committees.	6. The management body in its supervisory function should consider, taking into account the size and complexity of an institution, setting up specialized committees consisting of members of the management body (other persons may be invited to attend because their specific expertise or advice is relevant for a particular issue). Specialised committees may include an audit committee, a risk committee, a remuneration committee, a nomination or human resources committee and/or a governance or ethics or compliance committee.	Under the new Guidelines, , all institutions that are themselves significant, considering the individual, sub-consolidated and consolidated levels, must establish risk, nomination and remuneration committees to advise the Supervisory Board and to prepare the decisions to be taken by this Board. Under the old Guidelines, the Supervisory Board should consider, taking into account the size and complexity of an institution, setting up specialized committees consisting of members of the management body.
40. Where no risk or nomination committee is established, the references in these guidelines to those committees should be construed as applying to the management body in its supervisory function, taking into account the principle of proportionality as set out in Title I.		Where no risk or nomination committee is established, the references in these guidelines to those committees should be construed as applying to Supervisory Board, taking into account the principle of proportionality as set out in Title I.
41. Institutions may, taking into account the criteria set out in Title I of these guidelines, establish other committees (e.g. ethics, conduct and compliance committees).	6. The management body in its supervisory function should consider, taking into account the size and complexity of an institution, setting up specialized committees (…). Specialised committees may include (…) a governance or ethics or compliance committee.	No difference
42. Institutions should ensure a clear allocation and distribution of duties and tasks between specialised committees of the management		Under the new Guidelines, institutions should ensure a clear allocation and distribution of duties and tasks between specialised committees of the Supervisory

EBA Guidelines 2017	EBA Guidelines 2011	Differences
body.		Board.
43. Each committee should have a documented mandate, including the scope of its responsibilities, from the management body in its supervisory function and establish appropriate working procedures.	7. (…) Each committee should have a documented mandate (including its scope) from the management body in its supervisory function and established working procedures. (…).	
44. Committees should support the supervisory function in specific areas and facilitate the development and implementation of a sound internal governance framework. Delegating to committees does not in any way release the management body in its supervisory function from collectively fulfilling its duties and responsibilities.		Committees should support the Supervisory Board in specific areas and facilitate the development and implementation of a sound internal governance framework. Delegating to committees does not in any way release the Supervisory Board from collectively fulfilling its duties and responsibilities.
5.2 Composition of committees		
45. All committees should be chaired by a non-executive member of the management body who is able to exercise objective judgement.	7. A specialised committee should have an optimal mix of expertise, competencies and experience that, in combination, allows it to fully understand, objectively evaluate and bring fresh thinking to the relevant issues. It should have a sufficient number of independent members. (…) 10. The chair of the committee should be independent. If the chair is a former member of the management function of the institution, there should be an appropriate lapse of time before the position of committee chair is taken up.	Under the new Guidelines, all committees should be chaired by a non-executive member of the management body who is able to exercise objective judgement. Under Dutch law, the committees are chaired by a member of the Supervisory Board.
46. Independent members of the management body in its supervisory function should be actively involved in committees.		
47. Where committees have to be set up in		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
accordance with Directive 2013/36/EU or national law, they should be composed of at least three members.		
48. Institutions should ensure, taking into account the size of the management body and the number of independent members of the management body in its supervisory function, that committees are not composed of the same group of members that forms another committee.		
49. Institutions should consider the occasional rotation of chairs and members of committees, taking into account the specific experience, knowledge and skills that are individually or collectively required for those committees.	7. (…) Membership and chairmanship of a committee might be rotated occasionally.	
50. The risk and nomination committees should be composed of non-executive members of the management body in its supervisory function of the institution concerned. The audit committee should be composed in accordance with Article 41 of Directive 2006/43/EC. The remuneration committee should be composed in accordance with Section 2.4.1 of the EBA guidelines on sound remuneration policies.		The risk and nomination committees should be composed of non-executive members of the management body in its supervisory function of the institution concerned. The audit committee should be composed in accordance with Article 41 of Directive 2006/43/EC. The remuneration committee should be composed in accordance with Section 2.4.1 of the EBA guidelines on sound remuneration policies.
51. In G-SIIs and O-SIIs, the nomination committee should include a majority of members who are independent and be chaired by an independent member. In other significant institutions, determined by competent authorities or national law, the nomination committee should include a sufficient number of members who are independent; such institutions may also consider as a good		Under the new Guidelines, the nomination committee in Global Systemically Important Institutions (G-SIIs) and Other Systemically Important Institutions (O-SIIs) should include a majority of members who are independent and be chaired by an independent member.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
practice having a chair of the nomination committee who is independent.		
52. Members of the nomination committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning the selection process and suitability requirements.		
53. In G-SIIs and O-SIIs, the risk committee should include a majority of members who are independent. In G-SIIs and O-SIIs the chair of the risk committee should be an independent member. In other significant institutions, determined by competent authorities or national law, the risk committee should include a sufficient number of members who are independent and the risk committee should be chaired, where possible, by an independent member. In all institutions, the chair of the risk committee should be neither the chair of the management body nor the chair of any other committee.		Under the new Guidelines, the risk committee in G-SIIs and O-SIIs, should include a majority of members who are independent. In addition, the chair of the risk committee should be an independent member.
54. Members of the risk committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning risk management and control practices.		
5.3 Committees' processes		
55. Committees should regularly report to the management body in its supervisory function.	8. The respective committee chairs should report back regularly to the management body. (…)	No difference
56. Committees should interact with each other as appropriate. Without prejudice to paragraph 48, such interaction could take the form of cross-participation so that the chair or a	8. (…) The specialised committees should interact with each other as appropriate in order to ensure consistency and avoid any gaps. This could be done through cross-participation: the	No difference

EBA Guidelines 2017	EBA Guidelines 2011	Differences
member of a committee may also be a member of another committee.	chair or a member of one specialised committee might also be a member of another specialised committee	
57. Members of committees should engage in open and critical discussions, during which dissenting views are discussed in a constructive manner		
58. Committees should document the agendas of committee meetings and their main results and conclusions.		Under the new Guidelines, committees should document the agendas of committee meetings and their main results and conclusions.
59. The risk and nomination committees should at least: a. have access to all relevant information and data necessary to perform their role, including information and data from relevant corporate and control functions (e.g. legal, finance, human resources, IT, risk, compliance, audit, etc.); b. receive regular reports, ad hoc information, communications and opinions from heads of internal control functions concerning the current risk profile of the institution, its risk culture and its risk limits, as well as on any material breaches that may have occurred, with detailed information on and recommendations for corrective measures taken, to be taken or suggested to address them; c. periodically review and decide on the content, format and frequency of the information on risk to be reported to them; and d. where necessary, ensure the proper involvement of the internal control functions		The new Guidelines specify the ways in which the risk and nomination committees should be able to gather the necessary information to fulfil their tasks.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
and other relevant functions (human resources, legal, finance) within their respective areas of expertise and/or seek external expert advice.		
5.4 Role of the risk committee	*Risk committee*	
60. Where established, the risk committee should at least: a. advise and support the management body in its supervisory function regarding the monitoring of the institution's overall actual and future risk appetite and strategy, taking into account all types of risks, to ensure that they are in line with the business strategy, objectives, corporate culture and values of the institution; b. assist the management body in its supervisory function in overseeing the implementation of the institution's risk strategy and the corresponding limits set; c. oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of an institution, such as market, credit, operational (including legal and IT risks) and reputational risks, in order to assess their adequacy against the approved risk appetite and strategy; d. provide the management body in its supervisory function with recommendations on necessary adjustments to the risk strategy resulting from, inter alia, changes in the business model of the institution, market developments or recommendations made by	12. A risk committee (or equivalent) should be responsible for advising the management body on the institution's overall current and future risk tolerance/appetite and strategy, and for overseeing the implementation of that strategy. To enhance the effectiveness of the risk committee, it should regularly communicate with the institution's Risk Control function and Chief Risk Officer and should, where appropriate, have access to external expert advice, particularly in relation to proposed strategic transactions, such as mergers and acquisitions.	Under the new Guidelines, the role and responsibilities of the risk committee are further specified.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
the risk management function; e. provide advice on the appointment of external consultants that the supervisory function may decide to engage for advice or support; f. review a number of possible scenarios, including stressed scenarios, to assess how the institution's risk profile would react to external and internal events; g. oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the institution. The risk committee should assess the risks associated with the offered financial products and services and take into account the alignment between the prices assigned to and the profits gained from those products and services; and h. assess the recommendations of internal or external auditors and follow up on the appropriate implementation of measures taken.		
61. The risk committee should collaborate with other committees whose activities may have an impact on the risk strategy (e.g. audit and remuneration committees) and regularly communicate with the institution's internal control functions, in particular the risk management function.		Under the new Guidelines, it is specified that the risk committee should collaborate with other committee whose activities may have an impact on the risk strategy.
62. When established, the risk committee must, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration policies and practices take into consideration		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
the institution's risk, capital and liquidity and the likelihood and timing of earnings.		
5.5 Role of the audit committee	*Audit committee*	
63. In accordance with Directive 2006/43/EC19, where established, the audit committee should, inter alia: a. monitor the effectiveness of the institution's internal quality control and risk management systems and, where applicable, its internal audit function, with regard to the financial reporting of the audited institution, without breaching its independence; b. oversee the establishment of accounting policies by the institution; c. monitor the financial reporting process and submit recommendations aimed at ensuring its integrity; d. review and monitor the independence of the statutory auditors or the audit firms in accordance with Articles 22, 22a, 22b, 24a and 24b of Directive 2006/43/EU and Article 6 of Regulation (EU) No 537/2014, and in particular the appropriateness of the provision of non-audit services to the audited institution in accordance with Article 5 of that Regulation; e. monitor the statutory audit of the annual and consolidated financial statements, in particular its performance, taking into account any findings and conclusions by the competent authority pursuant to Article 26(6) of Regulation (EU) No 537/2014; f. be responsible for the procedure for the	9. An audit committee (or equivalent) should, inter alia, monitor the effectiveness of the company's internal control, internal audit, and risk management systems; oversee the institution's external auditors; recommend for approval by the management body the appointment, compensation and dismissal of the external auditors; review and approve the audit scope and frequency; review audit reports; and check that the management body in its management function takes necessary corrective actions in a timely manner to address control weaknesses, non-compliance with laws, regulations and policies, and other problems identified by the auditors. In addition, the audit committee should oversee the establishment of accounting policies by the institution. 11. Members of the audit committee as a whole should have recent and relevant practical experience in the area of financial markets or should have obtained, from their background business activities, sufficient professional 29 experience directly linked to financial markets activity. In any case, the chair of the audit committee should have specialist knowledge and experience in the application of accounting principles and internal control processes.	Under the new Guidelines, the role and responsibilities of the audit committee are further specified.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
selection of external statutory auditor(s) or audit firm(s) and recommend for approval by the institution's competent body their appointment (in accordance with Article 16 of Regulation (EU) No 537/2014 except when Article 16(8) of Regulation (EU) No 537/2014 is applied) compensation and dismissal; g. review the audit scope and frequency of the statutory audit of annual or consolidated accounts; h. in accordance with Article 39(6)(a) of Directive 2006/43/EU, inform the administrative or supervisory body of the audited entity of the outcome of the statutory audit and explain how the statutory audit contributed to the integrity of financial reporting and what the role of the audit committee was in that process; and i. receive and take into account audit reports.		
5.6 Combined committees		
64. In accordance with Article 76(3) of Directive 2013/36/EU, competent authorities may allow institutions that are not considered significant to combine the risk committee with, where established, the audit committee as referred to in Article 39 of Directive 2006/43/EC.		Under the new Guidelines, competent authorities may allow institutions that are not considered significant to combine the risk committee with, where established, the audit committee.
65. Where risk and nomination committees are established in non-significant institutions, they may combine the committees. If they do so, those institutions should document the reasons why they have chosen to combine the committees and how the approach achieves the		Under the new Guidelines, risk and nomination committees, where established, may be combined. In the event these committees are combined, institutions must document the reasons why they have chosen to combine the committees and how the approach achieves the objectives of the committees.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
objectives of the committees.		
66. Institutions should at all times ensure that the members of a combined committee possess, individually and collectively, the necessary knowledge, skills and expertise to fully understand the duties to be performed by the combined committee.		
Title III – Governance framework	***Title II – Requirements regarding institutions' internal governance***	
6 Organisational framework and structure	*A. Corporate Structure and Organisation*	
6.1 Organisational framework	4. Organisational framework	
67. The management body of an institution should ensure a suitable and transparent organisational and operational structure for that institution and should have a written description of it. The structure should promote and demonstrate the effective and prudent management of an institution at individual, sub consolidated and consolidated levels. The management body should ensure that the internal control functions are independent of the business lines they control, including that there is an adequate segregation of duties, and that they have the appropriate financial and human resources as well as powers to effectively perform their role. The reporting lines and the allocation of responsibilities, in particular among key function holders, within an institution should be clear, well-defined, coherent, enforceable and duly documented. The documentation should be updated as appropriate.	1. The management body of an institution shall ensure a suitable and transparent corporate structure for that institution. The structure shall promote and demonstrate the effective and prudent management of an institution both on a solo basis and at group level. The reporting lines and the allocation of responsibilities and authority within an institution shall be clear, well-defined, coherent and enforced. 2. The management body should ensure that the structure of an institution and, where applicable, the structures within a group are clear and transparent, both to the institution's own staff and to its supervisors.	The new Guidelines introduce the obligation for both the Executive and Supervisory Board to ensure that it has a written description of the organisational and operational structure of the institution. In addition, both the Executive and Supervisory Board should ensure that the internal control functions are independent of the business lines they control, including that there is an adequate segregation of duties, and that they have the appropriate financial and human resources as well as powers to effectively perform their role.
68. The structure of the institution should not	3. The management body should assess how the	No differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
impede the ability of the management body to oversee and manage effectively the risks the institution or the group faces or the ability of the competent authority to effectively supervise the institution.	various elements of the corporate 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.	
69. The management body should assess whether and how material changes to the group's structure (e.g. setting up of new subsidiaries, mergers and acquisitions, selling or winding-up parts of the group, or external developments) impact on the soundness of the institution's organisational framework. Where weaknesses are identified, the management body should make any necessary adjustments swiftly.	4. The management body should assess how changes to the group's structure impact on its soundness. The management body should make any necessary adjustments swiftly.	A minor difference in the sense that both the Executive and Supervisory Board should assess *whether* and how material changes to the group's structure impact on its soundness.
6.2 Know your structure	6. Know-your-structure	
70. The management body should fully know and understand the legal, organisational and operational structure of the institution ('know your structure') and ensure that it is in line with its approved business and risk strategy and risk appetite.	1. The management body shall fully know and understand the operational structure of an institution („know your structure") and ensure that it is in line with its approved business strategy and risk profile.	Both the Executive and Supervisory Board shall, under the new Guidelines, have full knowledge of not only the operational structure of the institution, but also the organisational and legal structure.
71. The management body should be responsible for the approval of sound strategies and policies for the establishment of new structures. Where an institution creates many legal entities within its group, their number and, in particular, the interconnections and transactions between them should not pose challenges for the design of its internal governance, and for the effective management and oversight of the risks of the group as a	2. (…) It [the management body] is also responsible for the approval of sound strategies and policies for the establishment of new structures.	Under the new guidelines, institutions should ensure that, where an institution creates many legal entities within its group, that their number and, in particular, the interconnections and transactions between them should not pose challenges for the design of its internal governance, and for the effective management and oversight of the risks of the group as a whole.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
whole. The management body should ensure that the structure of an institution and, where applicable, the structures within a group, taking into account the criteria specified in Section 7, are clear, efficient and transparent to the institution's staff, shareholders and other stakeholders and to the competent authority.		
72. The management body should guide the institution's structure, its evolution and its limitations and should ensure that the structure is justified and efficient and does not involve undue or inappropriate complexity.	2. The management body should guide and understand the institution's structure, its evolution and limitations and should ensure the structure is justified and does not involve undue or inappropriate complexity. (…)	No difference
73. The management body of a consolidating institution should understand not only the legal, organisational and operational structure of the group but also the purpose and activities of its different entities and the links and relationships among them. This includes understanding group specific operational risks and intra group exposures as well as how the group's funding, capital, liquidity and risk profiles could be affected under normal and adverse circumstances. The management body should ensure that the institution is able to produce information on the group in a timely manner, regarding the type, the characteristics, the organisational chart, the ownership structure and the businesses of each legal entity, and that the institutions within the group comply with all supervisory reporting requirements on an individual, sub-consolidated and consolidated basis.	3. The management body of an institution's parent company should understand not only the corporate organisation of the group but also the purpose 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 and risk profiles could be affected under normal and adverse circumstances. 4. The management body of an institution's parent company 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 aims and risks of the group. Any flow of significant information between entities relevant to the group's operational functioning should be documented and made accessible promptly, when requested, to the management body, the	In the new Guidelines it is specified that both the Executive and Supervisory Board of a consolidating institution should ensure that the institutions within the group comply with all supervisory reporting requirements on an individual, sub-consolidated and consolidated basis.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	control functions and supervisors, as appropriate.	
74. The management body of a consolidating institution should ensure that the different group entities (including the consolidating institution itself) receive enough information to get a clear perception of the general objectives, strategies and risk profile of the group and how the group entity concerned is embedded in the group's structure and operational functioning. Such information and revisions thereof should be documented and made available to the relevant functions concerned, including the management body, business lines and internal control functions. The members of the management body of a consolidating institution should keep themselves informed about the risks the group's structure causes, taking into account the criteria specified in Section 7 of the guidelines. This includes receiving: a. information on major risk drivers; b. regular reports assessing the institution's overall structure and evaluating the compliance of individual entities' activities with the approved group-wide strategy; and c. regular reports on topics where the regulatory framework requires compliance at individual, sub-consolidated and consolidated levels.	5. The management body of an institution's parent company should ensure it keeps itself informed about the risks the group's structure causes. This includes: a. information on major risk drivers, and b. regular reports assessing the institution's overall structure and evaluating individual entities'' activities compliance with the approved strategy.	Under the new Guidelines, both the Executive and Supervisory Board of a consolidating institution should ensure that the different group entities (including the consolidating institution itself) receive regular reports on topics where the regulatory framework requires compliance at individual, sub-consolidated and consolidated levels.
6.3 Complex structures and non-standard or non-transparent activities	7. Non-standard or non-transparent activities	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
75. Institutions should avoid setting up complex and potentially non transparent structures. Institutions should take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with money laundering or other financial crimes and the respective controls and legal framework in place. To this end, institutions should take into account at least: a. the extent to which the jurisdiction in which the structure will be set up complies effectively with EU and international standards on tax transparency, anti-money laundering and countering the financing of terrorism; b. the extent to which the structure serves an obvious economic and lawful purpose; c. the extent to which the structure could be used to hide the identity of the ultimate beneficial owner; d. the extent to which the customer's request that leads to the possible setting up of a structure gives rise to concern; e. whether the structure might impede appropriate oversight by the institution's management body or the institution's ability to manage the related risk; and f. whether the structure poses obstacles to effective supervision by competent authorities.		In the new Guidelines, it is specified that institutions should avoid setting up complex and potentially non-transparent structures. In addition, institutions should take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with money laundering or other financial crimes and the respective controls and legal framework in place. In the new Guidelines the different factors an institution should take into account in the aforementioned decision-making are specified. Further details on the assessment of country risk and the risk associated with individual products and customers, institutions should refer also to the final (once issued) joint guidelines on risk factors: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factorsand-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper .
76. In any case, institutions should not set up opaque or unnecessarily complex structures which have no clear economic rationale or		In any case, institutions should not set up opaque or unnecessarily complex structures which have no clear economic rationale or legal purpose or if institutions are

EBA Guidelines 2017	EBA Guidelines 2011	Differences
legal purpose or if institutions are concerned that these structures might be used for a purpose connected with financial crime.		concerned that these structures might be used for a purpose connected with financial crime.
77. When setting up such structures, the management body should understand them and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. Such structures should be approved and maintained only when their purpose has been clearly defined and understood, and when the management body is satisfied that all material risks, including reputational risks, have been identified, that all risks can be managed effectively and appropriately reported, and that effective oversight has been ensured. The more complex and opaque the organisational and operational structure, and the greater the risks, the more intensive the oversight of the structure should be.		Under the new Guidelines, both the Executive and Supervisory Board should understand complex and potential non-transparent structures and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. Such structures should be approved and maintained only when their purpose has been clearly defined and understood, and when the management body is satisfied that all material risks, including reputational risks, have been identified, that all risks can be managed effectively and appropriately reported, and that effective oversight has been ensured.
78. Institutions should document their decisions and be able to justify their decisions to competent authorities.		
79. The management body should ensure that appropriate actions are taken to avoid or mitigate the risks of activities within such structures. This includes ensuring that: a. the institution has in place adequate policies and procedures and documented processes (e.g. applicable limits, information requirements) for the consideration, compliance, approval and risk management of such activities, taking into	3. The management body should ensure appropriate actions are taken to avoid or mitigate the risks of such activities. This includes that: a. the institution has in place adequate policies and procedures and documented processes (e.g. applicable limits, information requirements) for the consideration, approval and risk management of such activities, taking into	Under the new Guidelines, both the Executive and Supervisory Board should ensure that information concerning these activities within the non-transparent structures and the risks thereof are reported to the competent authority that granted authorisation.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
account the consequences for the group's organisational and operational structure, its risk profile and its reputational risk; b. information concerning these activities and the risks thereof is accessible to the consolidating institution and internal and external auditors and is reported to the management body in its supervisory function and to the competent authority that granted authorisation; and c. the institution periodically assesses the continuing need to maintain such structures.	account the consequences for the group's operational structure; b. information concerning these activities and its risks is accessible to the institution's head office and auditors and is reported to the management body and supervisors; c. the institution periodically assesses the continuing need to perform activities that impede transparency.	
80. These structures and activities, including their compliance with legislation and professional standards, should be subject to regular review by the internal audit function following a risk-based approach.	5. All these structures and activities should be subject to periodic internal and external audit reviews.	Under the new Guidelines, it is specified that the periodic internal review should be based on a risk-based approach.
81. Institutions should take the same risk management measures as for the institution's own business activities when they perform non- standard or non-transparent activities for clients (e.g. helping clients to set up vehicles in offshore jurisdictions, developing complex structures, financing transactions for them or providing trustee services) that pose similar internal governance challenges and create significant operational and reputational risks. In particular, institutions should analyse the reason why a client wants to set up a particular structure.	4. The same measures should be taken when an institution performs nonstandard or non-transparent activities for clients.	Under the new Guidelines, institutions should analyse the reason why a client wants to set up a particular structure that could pose internal governance challenges and create significant operational and reputational risks
7 Organisational framework in a group context	5. Checks and balances in a group structure	
82. In accordance with Article 109(2) of Directive 2013/36/EU, parent undertakings and	1. In a group structure, the management body of an institution's parent company shall have the	Under the new Guidelines, parent undertakings and subsidiaries subject to CRD IV should ensure that

EBA Guidelines 2017	EBA Guidelines 2011	Differences
subsidiaries subject to that Directive should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated and sub-consolidated basis. To this end, parent undertakings and subsidiaries within the scope of prudential consolidation should implement such arrangements, processes and mechanisms in their subsidiaries not subject to Directive 2013/36/EU to ensure robust governance arrangements on a consolidated and sub-consolidated basis. Competent functions within the consolidating institution and its subsidiaries should interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms should ensure that the consolidating institution has sufficient data and information and is able to assess the group-wide risk profile, as detailed in Section 6.2.	overall responsibility for adequate internal governance across the group and for ensuring that there is a governance framework appropriate to the structure, business and risks of the group and its component entities.	governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated and sub-consolidated basis. To this end, parent undertakings and subsidiaries within the scope of prudential consolidation should implement such arrangements, processes and mechanisms in their subsidiaries not subject to CRD IV to ensure robust governance arrangements on a consolidated and sub-consolidated basis.
83. The management body of a subsidiary that is subject to Directive 2013/36/EU should adopt and implement on the individual level the group-wide governance policies established at the consolidated or sub-consolidated level, in a manner that complies with all specific requirements under EU and national law.	2. The management body of a regulated subsidiary of a group should adhere at the legal entity level to the same internal governance values and policies as its parent company, unless legal or supervisory requirements or proportionality considerations determine otherwise. Accordingly, the management body of a regulated subsidiary should within its own internal governance responsibilities, set its policies, and should evaluate any group-level decisions or practices to ensure that they do not put the regulated subsidiary in breach of applicable legal or regulatory provisions or	Under the new Guidelines, both the Executive and Supervisory Board of a subsidiary that is subject to CRD IV should adopt and implement on the individual level the group-wide governance policies established at the consolidated or sub-consolidated level, in a manner that complies with all specific requirements under EU and national law.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	prudential rules. The management body of the regulated subsidiary should also ensure that such decisions or practices are not detrimental to: a. the sound and prudent management of the subsidiary; b. the financial health of the subsidiary; or c. the legal interests of the subsidiary's stakeholders.	
84. At the consolidated and sub-consolidated levels, the consolidating institution should ensure adherence to the group-wide governance policies by all institutions and other entities within the scope of prudential consolidation, including their subsidiaries not themselves subject to Directive 2013/36/EU. When implementing governance policies, the consolidating institution should ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.	4. In discharging its internal governance responsibilities, the management body of an institution's parent company should be aware of all the material risks and issues that might affect the group, the parent institution itself and its subsidiaries. It should therefore exercise adequate oversight over its subsidiaries, while respecting the independent legal and governance responsibilities that apply to regulated subsidiaries‟ management bodies.	At the consolidated and sub-consolidated levels, the consolidating institution should ensure adherence to the group-wide governance policies by all institutions and other entities within the scope of prudential consolidation, including their subsidiaries not themselves subject to CRD IV.
85. A consolidating institution should consider the interests of all its subsidiaries, and how strategies and policies contribute to the interest of each subsidiary and the interest of the group as a whole over the long term.	5. In order to fulfil its internal governance responsibilities, the management body of an institution's parent company should: a. establish a governance structure which	A consolidating institution should, under the new Guidelines, consider the interests of all its subsidiaries, and how strategies and policies contribute to the interest of each subsidiary and the interest of the group as a whole over the long term.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	contributes to the effective oversight of its subsidiaries and takes into account the nature, scale and complexity of the different risks to which the group and its subsidiaries are exposed; b. approve an internal governance policy at the group level for its subsidiaries, which includes the commitment to meet all applicable governance requirements; c. ensure that enough resources are available for each subsidiary to meet both group standards and local governance standards; d. have appropriate means to monitor that each subsidiary complies with all applicable internal governance requirements; and e. ensure that reporting lines in a group should be clear and transparent, especially where business lines do not match the legal structure of the group.	
86. Parent undertakings and their subsidiaries should ensure that the institutions and entities within the group comply with all specific requirements in any relevant jurisdiction.	3. The management bodies of both the parent company and its subsidiaries should apply and take into account the paragraphs below, considering the effects of the group dimension on their internal governance.	No difference.
87. The consolidating institution should ensure that subsidiaries established in third countries, and which are included in the scope of prudential consolidation, have governance arrangements, processes and mechanisms in place that are consistent with group-wide governance policies and comply with the requirements of Articles 74 to 96 of Directive 2013/36/EU and these guidelines, as long as		Under the new Guidelines, the consolidating institution should ensure that subsidiaries established in third countries, and which are included in the scope of prudential consolidation, have governance arrangements, processes and mechanisms in place that are consistent with group-wide governance policies and comply with the requirements of Articles 74 to 96 of CRD IV and these guidelines, as long as this is not unlawful under the laws of the third country.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
this is not unlawful under the laws of the third country.		
88. The governance requirements of Directive 2013/36/EU and these guidelines apply to institutions independent of the fact that they may be subsidiaries of a parent undertaking in a third country. Where an EU subsidiary of a parent undertaking in a third country is a consolidating institution, the scope of prudential consolidation does not include the level of the parent undertaking located in a third country and other direct subsidiaries of that parent undertaking. The consolidating institution should ensure that the group-wide governance policy of the parent institution in a third country is taken into consideration within its own governance policy insofar as this is not contrary to the requirements set out under relevant EU law, including Directive 2013/36/EU and these guidelines.		In the new Guidelines it is specified that the governance requirements of CRD IV and these guidelines apply to institutions independent of the fact that they may be subsidiaries of a parent undertaking in a third country.
89. When establishing policies and documenting governance arrangements, institutions should take into account the aspects listed in Annex I to the guidelines. While policies and documentation may be included in separate documents, institutions should consider combining them or referring to them in a single governance framework document.		When establishing policies and documenting governance arrangements, institutions should take into account the aspects listed in Annex I to the guidelines.
8 Outsourcing policy	***B.4 Outsourcing and remuneration policies - 18. Outsourcing***	These guidelines are limited to the general outsourcing policy; specific aspects of the issue of outsourcing are dealt with in the CEBS guidelines on outsourcing, which are due to be revised. These guidelines are available at https://www.eba.europa.eu/regulation-and-

EBA Guidelines 2017	EBA Guidelines 2011	Differences
		policy/internal-governance/guidelines-on-outsourcing.
90. The management body should approve and regularly review and update the outsourcing policy of an institution, ensuring that appropriate changes are implemented in a timely manner.	1. The management body shall approve and regularly review the outsourcing policy of an institution. 2. (…) The policy should be reviewed and updated regularly, with changes to be implemented in a timely manner.	Under the new Guidelines, the management body has an explicit responsibility to ensure that the outsourcing policy is updated.
91. The outsourcing policy should consider the impact of outsourcing on an institution's business and the risks it faces (such as operational risks, including legal and IT risks; reputational risks; and concentration risks). The policy should include the reporting and monitoring arrangements to be implemented from inception to the end of an outsourcing agreement (including drawing up the business case for outsourcing, entering into an outsourcing contract, the implementation of the contract to its expiry, contingency plans and exit strategies). An institution remains fully responsible for all outsourced services and activities and management decisions arising from them. Accordingly, the outsourcing policy should make it clear that outsourcing does not relieve the institution of its regulatory obligations and its responsibilities to its customers.	2. 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 an 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 changes to be implemented in a timely manner. 3. 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.	Under the new Guidelines, the legal and IT risks connected to outsourcing are specified.
92. The policy should state that outsourcing	4. The policy should state that outsourcing	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
arrangements should not hinder effective on-site or off site supervision of the institution and should not contravene any supervisory restrictions on services and activities. The policy should also cover intragroup outsourcing (i.e. services provided by a separate legal entity within an institution's group) and take into account any specific group circumstances.	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 internal outsourcing (e.g. by a separate legal entity within an institution's group) and any specific group circumstances to be taken into account.	
93. The policy should require that, when selecting material external services providers or when outsourcing activities, the institution must take into account whether or not the service provider has in place appropriate ethical standards or a code of conduct.		
	19. Governance of remuneration policy	The Guidelines regarding the governance of the remuneration policy are repealed. These provisions are part of the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013 (EBA/GL/2015/22).
	1. Ultimate oversight of the remuneration policy shall rest with an institution's management body.	
	2. The management body in its supervisory function should maintain, approve and oversee the principles of the overall remuneration policy for its institution. The institution's procedures for determining remuneration should be clear, well documented and internally transparent.	
	3. In addition to the management body's general responsibility for the overall remuneration	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	policy and its review, adequate involvement of the control functions is required. Members of the management body, members of the remuneration committee and other staff members who are involved in the design and implementation of the remuneration policy should have relevant expertise and be capable of forming an independent judgement on the suitability of the remuneration policy, including its implications for risk management.	
	4. The remuneration policy should also be aimed at preventing conflicts of interest. The management body in its management function should not determine its own remuneration; to avoid doing so, it might consider, for example, using an independent remuneration committee. A business unit should not be able to determine the remuneration of its control functions.	
	5. The management body should maintain oversight of the application of the remuneration policy to ensure it works as intended. The implementation of the remuneration policy should also be subject to central and independent review.	
Title IV – Risk culture and business conduct	***C. Risk management***	
9 Risk culture	*20. Risk culture*	
95. Institutions should develop an integrated and institution-wide risk culture, based on a full understanding and holistic view of the risks they face and how they are managed, taking into account the institution's risk appetite.	1. An institution shall develop an integrated and institution-wide risk culture, based on a full understanding of the risks it faces and how they are managed, taking into account its risk tolerance/appetite.	Under the new Guidelines, it is specified that the risk culture should *inter alia* be based on a holistic view of the risks the institution faces.
96. Institutions should develop a risk culture through policies, communication and staff	2. An institution should develop its risk culture through policies, examples, communication and	No differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
training regarding the institutions' activities, strategy and risk profile, and should adapt communication and staff training to take into account staff's responsibilities regarding risk-taking and risk management.	training of staff regarding their responsibilities for risk.	
97. Staff should be fully aware of their responsibilities relating to risk management. Risk management should not be confined to risk specialists or internal control functions. Business units, under the oversight of the management body, should be primarily responsible for managing risks on a day-to-day basis in line with the institution's policies, procedures and controls, taking into account the institution's risk appetite and risk capacity.	3. Every member of the organisation should be fully aware of his or her responsibilities relating to risk management. Risk management should not be confined to risk specialists or 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 tolerance/appetite and in line with its policies, procedures and controls.	No differences.
98. A strong risk culture should include but is not necessarily limited to: a. Tone from the top: the management body should be responsible for setting and communicating the institution's core values and expectations. The behaviour of its members should reflect the values being espoused. Institutions' management, including key function holders, should contribute to the internal communication of core values and expectations to staff. Staff should act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance within or outside the institution (e.g. to the competent authority through a whistleblowing process). The		Under the new Guidelines, some important factors that should be included in the risk culture are specified, such as the responsibility of the management body for setting and communicating the institution's core values and expectations. See also the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013 (EBA/GL/2015/22), available at https://www.eba.europa.eu/regulation-and-policy/remuneration.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
management body should on an ongoing basis promote, monitor and assess the risk culture of the institution; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the institution; and make changes where necessary. b. Accountability: relevant staff at all levels should know and understand the core values of the institution and, to the extent necessary for their role, its risk appetite and risk capacity. They should be capable of performing their roles and be aware that they will be held accountable for their actions in relation to the institution's risk-taking behaviour. c. Effective communication and challenge: a sound risk culture should promote an environment of open communication and effective challenge in which decision-making processes encourage a broad range of views, allow for testing of current practices, stimulate a constructive critical attitude among staff, and promote an environment of open and constructive engagement throughout the entire organisation. d. Incentives: appropriate incentives should play a key role in aligning risk-taking behaviour with the institution's risk profile and its long-term interest.		
10 Corporate values and code of conduct	*B.3 Framework for business conduct - 15. Corporate values and code of conduct*	
99. The management body should develop, adopt, adhere to and promote high ethical and professional standards, taking into account the	1. The management body shall develop and promote high ethical and professional standards.	Under the new Guidelines, it is specified that the both the Executive and Supervisory Board should develop, adopt, adhere to and promote high ethical and professional

EBA Guidelines 2017	EBA Guidelines 2011	Differences
specific needs and characteristics of the institution, and should ensure the implementation of such standards (through a code of conduct or similar instrument). It should also oversee adherence to these standards by staff. Where applicable, the management body may adopt and implement the institution's group-wide standards or common standards released by associations or other relevant organisations.		standards, taking into account the specific needs and characteristics of the institution, and should ensure the implementation of such standards (through a code of conduct or similar instrument).
100. The implemented standards should aim to reduce the risks to which the institution is exposed, in particular operational and reputational risks, which can have a considerable adverse impact on an institution's profitability and sustainability through fines, litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties ,and the loss of brand value and consumer confidence.		The implemented standards should aim to reduce the risks to which the institution is exposed, in particular operational and reputational risks, which can have a considerable adverse impact on an institution's profitability and sustainability through fines, litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties ,and the loss of brand value and consumer confidence.
101. The management body should have clear and documented policies for how these standards should be met. These policies should: a. remind readers that all the institution's activities should be conducted in compliance with the applicable law and with the institution's corporate values; b. promote risk awareness through a strong risk culture in line with Section 9 of the guidelines, conveying the management body's expectation that activities will not go beyond the defined risk appetite and limits defined by the	2. The management body should have clear policies for how these standards should be met.	Under the new Guidelines, the content of the business conduct policies is specified.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
institution and the respective responsibilities of staff; c. set out principles on and provide examples of acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, economic and financial crime (including fraud, money laundering and anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws); d. clarify that in addition to complying with legal and regulatory requirements and internal policies, staff are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; and e. ensure that staff are aware of the potential internal and external disciplinary actions, legal actions and sanctions that may follow misconduct and unacceptable behaviours.		
102. Institutions should monitor compliance with such standards and ensure staff awareness, e.g. by providing training. Institutions should define the function responsible for monitoring compliance with and evaluating breaches of the code of conduct or similar instrument and a process for dealing with issues of non-compliance. The results should periodically be reported to the management body.	3. A continuing review of their implementation and the compliance with those standards should be performed. The results should be reported to the management body on a regular basis.	Under the new Guidelines, institutions should define the function responsible for monitoring compliance with and evaluating breaches of the code of conduct or similar instrument and a process for dealing with issues of non-compliance.
11 Conflict of interest policy at institutional level	*16. Conflicts of interest at institution level*	
103. The management body should be		Under the new Guidelines, the Executive Board should

EBA Guidelines 2017	EBA Guidelines 2011	Differences
responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at institutional level, e.g. as a result of the various activities and roles of the institution, of different institutions within the scope of prudential consolidation or of different business lines or units within an institution, or with regard to external stakeholders.		be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at an institutional level, e.g. as a result of the various activities and roles of the institution, of different institutions within the scope of prudential consolidation or of different business lines or units within an institution, or with regard to external stakeholders. In a two-tier model, the Executive Board should be responsible for establishing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at an institutional level, whereas the Supervisory Board should oversee the implementation and maintenance of these policies. Here again, the phrasing of the Guideline ponders the question if the Guidelines entails a right of approval for the Supervisory Board.
104. Institutions should take, within their organisational and administrative arrangements, adequate measures to prevent conflicts of interest from adversely affecting the interests of its clients.		
105. Institutions' measures to manage or where appropriate mitigate conflicts of interest should be documented and include, inter alia: a. an appropriate segregation of duties, e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
supervisory and reporting responsibilities for conflicting activities to different persons; b. establishing information barriers, e.g. through the physical separation of certain business lines or units; and c. establishing adequate procedures for transactions with related parties, e.g. requiring transactions to be conducted at arm's length.		
12 Conflict of interest policy for staff		This section should be read in conjunction with the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.
106. The management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts between the interests of the institution and the private interests of staff, including members of the management body, which could adversely influence the performance of their duties and responsibilities. A consolidating institution should consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.	1. The management body shall establish, implement and maintain effective policies to identify actual and potential conflicts of interest. Conflicts of interest that have been disclosed to and approved by the management body shall be appropriately managed.	In the new Guidelines, it is specified that a consolidating institution should consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.
107. The policy should aim to identify conflicts of interest of staff, including the interests of their closest family members. Institutions should take into consideration that conflicts of interest may arise not only from present but also from past personal or professional	2. A written policy should identify the relationships, services, activities or transactions of an institution in which conflicts of interest may arise and shall state how these conflicts should be managed. This policy should cover relationships and transactions between different	No material differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
relationships. Where conflicts of interest arise, institutions should assess their materiality and decide on and implement as appropriate mitigating measures.	clients of an institution and those between an institution and: a. its customers (as a result of the commercial model and/or the various services and activities provided by the institution); b. its shareholders; c. the members of its management body; d. its staff; e. significant suppliers or business partners; and f. other related parties (e.g. its parent company or subsidiaries).	
108. Regarding conflicts of interest that may result from past relationships, institutions should set an appropriate timeframe for which they want staff to report such conflicts of interest, on the basis that these may still have an impact on staff's behaviour and participation in decision-making.		
109. The policy should cover at least the following situations or relationships where conflicts of interest may arise: a. economic interests (e.g. shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the institution to a company owned by staff, membership in a body or ownership of a body or entity with conflicting interests); b. personal or professional relationships with the owners of qualifying holdings in the institution;	3. A parent company should consider and balance the interests of all its subsidiaries, and consider how these interests contribute to the common purpose and interests of the group as a whole over the long term.	The specific situations a conflict of interest policy should cover is further specified in the new Guidelines. The policy should cover at least: a. economic interests (e.g. shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the institution to a company owned by staff, membership in a body or ownership of a body or entity with conflicting interests); b. personal or professional relationships with the owners of qualifying holdings in the institution; c. personal or professional relationships with staff of the institution or entities included within the scope of

EBA Guidelines 2017	EBA Guidelines 2011	Differences
c. personal or professional relationships with staff of the institution or entities included within the scope of prudential consolidation (e.g. family relationships); d. other employment and previous employment within the recent past (e.g. five years); e. personal or professional relationships with relevant external stakeholders (e.g. being associated with material suppliers, consultancies or other service providers); and f. political influence or political relationships.		prudential consolidation (e.g. family relationships); d. other employment and previous employment within the recent past (e.g. five years); e. personal or professional relationships with relevant external stakeholders (e.g. being associated with material suppliers, consultancies or other service providers); and f. political influence or political relationships.
110. Notwithstanding the above, institutions should take into consideration that being a shareholder of an institution or having private accounts or loans with or using other services of an institution should not lead to a situation where staff are considered to have a conflict of interest if they stay within an appropriate de minimis threshold.		
111. The policy should set out the processes for reporting and communication to the function responsible under the policy. Staff should have the duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest.		The policy should set out the processes for reporting and communication to the function responsible under the policy. Staff should have the duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest.
112. The policy should differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur unexpectedly with regard to a single event (e.g. a transaction, the selection of service provider, etc.) and can usually be managed with a one-off measure. In all circumstances, the interest of the institution		The policy should differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur unexpectedly with regard to a single event (e.g. a transaction, the selection of service provider, etc.) and can usually be managed with a one-off measure. In all circumstances, the interest of the institution should be central to the decisions taken.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
should be central to the decisions taken.		
113. The policy should set out procedures, measures, documentation requirements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures. Such procedures, requirements, responsibilities and measures should include: a. entrusting conflicting activities or transactions to different persons; b. preventing staff who are also active outside the institution from having inappropriate influence within the institution regarding those other activities; c. establishing the responsibility of the members of the management body to abstain from voting on any matter where a member has or may have a conflict of interest or where the member's objectivity or ability to properly fulfil duties to the institution may be otherwise compromised; d. establishing adequate procedures for transactions with related parties (institutions may consider, inter alia, requiring transactions to be conducted at arm's length, requiring that all relevant internal control procedures fully apply to such transactions, requiring binding consultative advice from independent members of the management body, requiring the approval by shareholders of the most relevant transactions and limiting exposure to such	4. The conflict of interest policy should set out measures to be adopted to prevent or manage conflicts of interest. Such procedures and measures might include: a. 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; and c. preventing people who are also active outside the institution from having inappropriate influence within the institution regarding those activities.	In the new Guidelines it is specified that the policy should set out documentation requirements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
transactions); and e. preventing members of the management body from holding directorships in competing institutions, unless they are within institutions that belong to the same institutional protection scheme, as referred to in Article 113(7) of Regulation (EU) No 575/2013, credit institutions permanently affiliated to a central body, as referred to in Article 10 of Regulation (EU) No 575/2013, or institutions within the scope of prudential consolidation.		
114. The policy should specifically cover the risk of conflicts of interest at the level of the management body and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of members of the management body to take objective and impartial decisions that aim to fulfil the best interests of the institution. Institutions should take into consideration that conflicts of interest can have an impact on the independence of mind of members of the management body.		The new Guidelines also specify that the conflict of interest policy should specifically cover the risk of conflicts of interest at the level of the management body and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of members of the management body to take objective and impartial decisions that aim to fulfil the best interests of the institution. See also the Joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.
115. Actual or potential conflicts of interest that have been disclosed to the responsible function within the institution should be appropriately assessed and managed. If a conflict of interest of staff is identified, the institution should document the decision taken, in particular if the conflict of interest and the related risks have been accepted, and if it has		Under the new Guidelines, actual or potential conflicts of interest that have been disclosed to the responsible function within the institution should be appropriately assessed and managed

EBA Guidelines 2017	EBA Guidelines 2011	Differences
been accepted, how this conflict of interest has been satisfactorily mitigated or remedied.		
116. All actual and potential conflicts of interest at management body level, individually and collectively, should be adequately documented, communicated to the management body, and discussed, decided on and duly managed by the management body.		Under the new Guidelines, all actual and potential conflicts of interest at management body level, individually and collectively, should be adequately documented, communicated to the management body, and discussed, decided on and duly managed by the management body
13 Internal alert procedures	*17. Internal alert procedures*	
117. Institutions should put in place and maintain appropriate internal alert policies and procedures for staff to report potential or actual breaches of regulatory or internal requirements, including, but not limited to, those of Regulation (EU) No 575/2013 and national provisions transposing Directive 2013/36/EU, or of internal governance arrangements, through a specific, independent and autonomous channel. It should not be necessary for reporting staff to have evidence of a breach; however, they should have a sufficient level of certainty that provides sufficient reason to launch an investigation.	1. The management body shall put in place appropriate internal alert procedures for communicating internal governance concerns from the staff. 2. An institution should adopt appropriate internal alert procedures that staff can use to draw attention to significant and legitimate concerns regarding matters connected with internal governance. (…).	No differences
118. To avoid conflicts of interest, it should be possible for staff to report breaches outside regular reporting lines (e.g. through the compliance function, the internal audit function or an independent internal whistleblowing procedure). The alert procedures should ensure the protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Directive 95/46/EC.	2. (…) These procedures should respect the confidentiality of the staff that raises such concerns. To avoid conflicts of interest there should be an opportunity to raise these kinds of concerns outside regular reporting lines (e.g. through the Compliance function or the Internal Audit function or an internal whistle-blower procedure). (…)	No differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
119. The alert procedures should be made available to all staff within an institution.	2. (…)The alert procedures should be made available to all staff within an institution (…).	
120. Information provided by staff through the alert procedures should, if appropriate, be made available to the management body and other responsible functions defined within the internal alert policy. Where required by the staff member reporting a breach, the information should be provided to the management body and other responsible functions in an anonymised way. Institutions may also provide for a whistleblowing process that allows information to be submitted in an anonymised way.	2. (…)Information provided by the staff via the alert procedure should, if relevant, be made available to the management body.	In the new Guidelines, it is specified that the information provided by staff through the alert procedures should, if appropriate, be made available not only to the management body, but also to the other responsible functions defined within the internal alert policy.
121. Institutions should ensure that the person reporting the breach is appropriately protected from any negative impact, e.g. retaliation, discrimination or other types of unfair treatment. The institution should ensure that no person under the institution's control engages in victimisation of a person who has reported a breach and should take appropriate measures against those responsible for any such victimisation.		Institutions should, under the new Guidelines, ensure that the person reporting the breach is appropriately protected from any negative impact, e.g. retaliation, discrimination or other types of unfair treatment.
122. Institutions should also protect persons who have been reported from any negative effects in case the investigation finds no evidence that justifies taking measures against that person. If measures are taken, the institution should take them in a way that aims to protect the person concerned from unintended negative effects that go beyond the objective of the measure taken.		Institutions also have the obligation to protect persons who have been reported from any negative effects in case the investigation finds no evidence that justifies taking measures against that person under the new Guidelines.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
123. In particular, internal alert procedures should: a. be documented (e.g. staff handbooks); b. provide clear rules that ensure that information on the reporting and the reported persons and the breach are treated confidentially, in accordance with Directive 95/46/EC, unless disclosure is required under national law in the context of further investigations or subsequent judicial proceedings; c. protect staff who raise concerns from being victimised because they have disclosed reportable breaches; d. ensure that the potential or actual breaches raised are assessed and escalated, including as appropriate to the relevant competent authority or law enforcement agency; e. ensure, where possible, that confirmation of receipt of information is provided to staff who have raised potential or actual breaches; f. ensure the tracking of the outcome of an investigation into a reported breach; and g. ensure appropriate record keeping.		The new Guidelines specify what the internal alert procedures should entail.
14 Reporting of breaches to competent authorities		
124. Competent authorities should establish effective and reliable mechanisms to enable institutions' staff to report to competent authorities relevant potential or actual breaches of regulatory requirements, including, but not limited to, those of Regulation (EU) No		Under the new Guidelines, competent authorities have the responsibility to establish effective and reliable mechanisms to enable institutions' staff to report to competent authorities relevant potential or actual breaches of regulatory requirements.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
575/2013 and national provisions transposing Directive 2013/36/EU. These mechanisms should include at least: a. specific procedures for the receipt of reports on breaches and follow up, for instance a dedicated whistleblowing department, unit or function; b. appropriate protection as referred to in Section 13; c. protection of the personal data of both the natural person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Directive 95/46/EC; and d. clear procedures as set out in paragraph 123.		
125. Without prejudice to the possibility of reporting breaches through the competent authorities' mechanisms, competent authorities may encourage staff to first try and seek to use their institutions' internal alert procedures.		Without prejudice to the possibility of reporting breaches through the competent authorities' mechanisms, competent authorities may encourage staff to first try and seek to use their institutions' internal alert procedures.
Title V – Internal control framework and mechanisms		
15 Internal control framework		
126. Institutions should develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the institution and a robust and comprehensive internal control framework. Under this framework, institutions' business lines should be responsible for managing the risks they incur in conducting their activities and should have controls in place that aim to ensure		Under the new Guidelines, institutions should develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the institution and a robust and comprehensive internal control framework.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
compliance with internal and external requirements. As part of this framework, institutions should have internal control functions with appropriate and sufficient authority, stature and access to the management body to fulfil their mission, and a risk management framework.		
127. The internal control framework of the institution concerned should be adapted on an individual basis to the specificity of its business, its complexity and the associated risks, taking into account the group context. The institutions concerned must organise the exchange of the information necessary in a manner that ensures that each management body, business line and internal unit, including each internal control function, is able to carry out its duties. This means, for example, a necessary exchange of adequate information between the business lines and the compliance function at the group level and between the heads of the internal control functions at the group level and the management body of the institution.		This internal control framework should be adapted to the specificity of its business, its complexity and the associated risks, taking into account the group context.
128. The internal control framework should cover the whole organisation, including the management body's responsibilities and tasks, and the activities of all business lines and internal units, including internal control functions, outsourced activities and distribution channels.		The internal control framework should cover the whole organisation, including the management body's responsibilities and tasks, and the activities of all business lines and internal units, including internal control functions, outsourced activities and distribution channels.
129. The internal control framework of an institution should ensure:		The new Guidelines specify some further requirements regarding the internal control framework.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
a. effective and efficient operations; b. prudent conduct of business; c. adequate identification, measurement and mitigation of risks; d. the reliability of financial and non-financial information reported both internally and externally; e. sound administrative and accounting procedures; and f. compliance with laws, regulations, supervisory requirements and the institution's internal policies, processes, rules and decisions.		
16 Implementing an internal control framework		
130. The management body should be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework, processes and mechanisms, and for overseeing all business lines and internal units, including internal control functions (such as risk management, compliance and internal audit functions). Institutions should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures, which should be approved by the management body.		Under the new Guidelines, the management body should be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework, processes and mechanisms, and for overseeing all business lines and internal units, including internal control functions (such as risk management, compliance and internal audit functions).
131. An institution should have a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority within its internal control framework, including its business lines,		In the new Guidelines, it is specified that an institution should have a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority within its internal control framework, including its business lines, internal units and

EBA Guidelines 2017	EBA Guidelines 2011	Differences
internal units and internal control functions.		internal control functions.
132. Institutions should communicate those policies, mechanisms and procedures to all staff and every time material changes have been made.		Institutions are under the new Guidelines also required communicate those policies, mechanisms and procedures to all staff and every time material changes have been made.
133. When implementing the internal control framework, institutions should establish adequate segregation of duties – e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons – and establish information barriers, e.g. through the physical separation of certain departments.		Institutions are also required to establish an adequate segregation of duties – e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons – and establish information barriers, e.g. through the physical separation of certain departments, when implementing the internal control framework.
134. The internal control functions should verify that the policies, mechanisms and procedures set out in the internal control framework are correctly implemented in their respective areas of competence.		The internal control functions should verify that the policies, mechanisms and procedures set out in the internal control framework are correctly implemented in their respective areas of competence.
135. Internal control functions should regularly submit to the management body written reports on major identified deficiencies. These reports should include, for each new identified major deficiency, the relevant risks involved, an impact assessment, recommendations and corrective measures to be taken. The management body should follow up on the findings of the internal control functions in a timely and effective manner and require adequate remedial actions. A formal follow-up procedure on findings and corrective measures taken should be put in place.		Internal control functions should regularly submit to the Executive and the Supervisory Board written reports on major identified deficiencies.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
17 Risk management framework	*C. Risk Management - 20. Risk Culture*	
136. As part of the overall internal control framework, institutions should have a holistic institution wide risk management framework extending across all its business lines and internal units, including internal control functions, recognising fully the economic substance of all its risk exposures. The risk management framework should enable the institution to make fully informed decisions on risk-taking. The risk management framework should encompass on- and off-balance-sheet risks as well as actual risks and future risks that the institution may be exposed to. Risks should be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the institution and at consolidated or sub-consolidated level. All relevant risks should be encompassed in the risk management framework with appropriate consideration of both financial and non-financial risks, including credit, market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance and strategic risks.	4. An institution should have a holistic risk management framework extending across all its business, support and control units, recognizing fully the economic substance of its risk exposures and encompassing all relevant risks (e.g. financial and non-financial, on and off balance sheet, and whether or not contingent or contractual). Its scope should not be limited to credit, market, liquidity and operational risks, but should also include concentration, reputational, compliance and strategic risks. 5. The risk management framework should enable the institution to make informed decisions. They should be based on information derived from identification, measurement or assessment and monitoring of risks. Risks should be evaluated bottom up and top down, through the management chain as well as across business lines, using consistent terminology and compatible methodologies throughout the institution and its group.	No differences.
	22. Risk management framework	
137. An institution's risk management framework should include policies, procedures, risk limits and risk controls ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the	1. An institution's risk management framework shall include policies, procedures, limits and controls providing adequate, timely and continuous identification, measurement or assessment, monitoring, mitigation and reporting of the risks posed by its activities at	No differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
risks at the business line, institution and consolidated or sub-consolidated levels.	the business line and institution-wide levels.	
138. An institution's risk management framework should provide specific guidance on the implementation of its strategies. This guidance should, where appropriate, establish and maintain internal limits consistent with the institution's risk appetite and commensurate with its sound operation, financial strength, capital base and strategic goals. An institution's risk profile should be kept within these established limits. The risk management framework should ensure that, whenever breaches of risk limits occur, there is a defined process to escalate and address them with an appropriate follow-up procedure.	2. An institution's risk management framework should provide specific guidance on the implementation of its strategies. They should, where appropriate, establish and maintain internal limits consistent with its risk tolerance/appetite and commensurate with its sound operation, financial strength and strategic goals. An institution's risk profile (i.e. the aggregate of its actual and potential risk exposures) should be kept within these limits. The risk management framework should ensure that breaches of the limits are escalated and addressed with appropriate follow up procedure	No differences
139. The risk management framework should be subject to independent internal review, e.g. performed by the internal audit function, and reassessed regularly against the institution's risk appetite, taking into account information from the risk management function and, where established, the risk committee. Factors that should be considered include internal and external developments, including balance-sheet and revenue changes; any increase in the complexity of the institution's business, risk profile or operating structure; geographic expansion; mergers and acquisitions; and the introduction of new products or business lines.	20.6. The risk management framework should be subject to independent internal or external review and reassessed regularly against the institution's risk tolerance/appetite, taking into account information from the Risk Control function and, where relevant, the risk committee. Factors that should be considered include internal and external developments, including balance sheet and revenue growth, 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.	No differences
140. When identifying and measuring or assessing risks, an institution should develop	3. When identifying and measuring risks, an institution should develop	The new Guidelines specify that institutions should make appropriately conservative assumptions when building

EBA Guidelines 2017	EBA Guidelines 2011	Differences
appropriate methodologies including both forward-looking and backward-looking tools. The methodologies should allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations. The tools should include the assessment of the actual risk profile against the institution's risk appetite, as well as the identification and assessment of potential and stressed risk exposures under a range of assumed adverse circumstances against the institution's risk capacity. The tools should provide information on any adjustment to the risk profile that may be required. Institutions should make appropriately conservative assumptions when building stressed scenarios.	forward-looking and backward-looking tools to complement work on current exposures. The tools should allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations. 4. Forward-looking tools (such as scenario analysis and stress tests) should identify potential risk exposures under a range of adverse circumstances; backward-looking tools should help review the actual risk profile against the institution's risk tolerance/appetite and its risk management framework and provide input for any adjustment.	stressed scenarios.
141. Institutions should take into consideration that the results of quantitative assessment methodologies, including stress testing, are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). For example, models showing very high returns on economic capital may result from a weakness in the models (e.g. the exclusion of some relevant risks) rather than a superior strategy or excellent execution of a strategy on the part of the institution. The determination of the level of risk taken should not therefore be based only on quantitative information or model outputs; it should also comprise a qualitative approach (including expert judgement and critical analysis).		Under the new Guidelines, institutions should take into consideration that the results of quantitative assessment methodologies, including stress testing, are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). For example, models showing very high returns on economic capital may result from a weakness in the models (e.g. the exclusion of some relevant risks) rather than a superior strategy or excellent execution of a strategy on the part of the institution. The determination of the level of risk taken should not therefore be based only on quantitative information or model outputs; it should also comprise a qualitative approach (including expert judgement and critical analysis). Relevant macroeconomic environmental trends and data should be explicitly addressed to identify their potential impact on exposures and portfolios

EBA Guidelines 2017	EBA Guidelines 2011	Differences
Relevant macroeconomic environmental trends and data should be explicitly addressed to identify their potential impact on exposures and portfolios.		
142. The ultimate responsibility for risk assessment lies solely with the institution, which, accordingly, should evaluate its risks critically and should not rely exclusively on external assessments. For example, an institution should validate a purchased risk model and calibrate it to its own individual circumstances to ensure that the model accurately and comprehensively captures and analyses the risk.	5. The ultimate responsibility for risk assessment lies solely with an institution which accordingly should evaluate its risks critically and should not exclusively rely on external assessments.	No difference.
143. Institutions should be fully aware of the limitations of models and metrics and use not only quantitative but also qualitative risk assessment tools (including expert judgement and critical analysis).	6. 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 judgement 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 formally integrated into material risk decisions.	No material difference.
144. In addition to the institutions' own assessments, institutions may use external risk assessments (including external credit ratings or externally purchased risk models). Institutions should be fully aware of the exact scope of such assessments and their limitations.		In the new Guidelines, it is specified that, in addition to the institutions' own assessments, institutions may use external risk assessments (including external credit ratings or externally purchased risk models). Institutions should be fully aware of the exact scope of such assessments and their limitations.
145. Regular and transparent reporting	7. Regular and transparent reporting	No difference.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
mechanisms should be established so that the management body, its risk committee, where established, and all relevant units in an institution are provided with reports in a timely, accurate, concise, understandable and meaningful manner and can share relevant information about the identification, measurement or assessment, monitoring and management of risks. The reporting framework should be well defined and documented.	mechanisms should be established so that the management body 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 approved by the management body.	
146. Effective communication and awareness regarding risks and the risk strategy is crucial for the whole risk management process, including the review and decision-making processes, and helps prevent decisions that may unknowingly increase risk. Effective risk reporting involves sound internal consideration and communication of risk strategy and relevant risk data (e.g. exposures and key risk indicators), both horizontally across the institution and up and down the management chain.	8. If a risk committee has been set up it should receive regularly formal reports and informal communication as appropriate from the Risk Control function and the Chief Risk Officer.	The new Guidelines specify some aspects of risk reporting. The old provision concerning reporting and communicating between the risk committee and the RCF/CRO has been repealed. Provisions regarding these reporting lines can be found in the specific provisions on the functioning of the risk committee.
	21. Alignment of remuneration with risk profile	The Guidelines regarding the governance of the remuneration policy are repealed. These provisions are part of the EBA guidelines on sound remuneration policies under Articles 74(3) and 75(2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013 (EBA/GL/2015/22). Also, some provisions of the new Guidelines refer to the relation between remuneration and the risk profile of the institution.
	1. An institution's remuneration policy and practices shall be consistent with its risk profile	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	and promote sound and effective risk management.	
	2. An institution's overall remuneration policy should be in line with its values, business strategy, risk tolerance/appetite and long-term interests. It should not encourage excessive risk-taking. Guaranteed variable remuneration or severance payments that end up rewarding failure are not consistent with sound risk management or the pay-for-performance principle and should, as a general rule, be prohibited.	
	3. For staff whose professional activities have a material impact on the risk profile of an institution (e.g. management body members, senior management, risk-takers in business units, staff responsible for internal control and any employee receiving total remuneration that takes them into the same remuneration bracket as senior management and risk takers), the remuneration policy should set up specific arrangements to ensure their remuneration is aligned with sound and effective risk management.	
	4. Control functions staff should be adequately compensated in accordance with their objectives and performance and not in relation to the performance of the business units they control.	
	5. Where the pay award is performance related, the remuneration should be based on a combination of individual and collective performance. When defining individual	

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	performance, factors other than financial performance should be considered. The measurement of performance for bonus awards should include adjustments for all types of risk and the cost of capital and liquidity.	
	6. There should be a proportionate ratio between basic pay and bonus. A significant bonus should not just be an up-front cash payment but should contain a flexible and deferred risk-adjusted component. The timing of the bonus payment should take into account the underlying risk performance.	
18 New products and significant changes	*23. New products*	See also EBA guidelines on product oversight and governance requirements for manufacturers and distributors of retail banking products..
147. An institution should have in place a well-documented new product approval policy (NPAP), approved by the management body, that addresses the development of new markets, products and services, and significant changes to existing ones, as well as exceptional transactions. The policy should in addition encompass material changes to related processes (e.g. new outsourcing arrangements) and systems (e.g. IT change processes). The NPAP should ensure that approved products and changes are consistent with the risk strategy and risk appetite of the institution and the corresponding limits, or that necessary revisions are made.	1. An institution shall have in place a well-documented new product approval policy ('NPAP'), approved by the management body, which addresses the development of new markets, products and services and significant changes to existing ones.	Under the new Guidelines, the new product approval policy (the NPAP) should encompass material changes to related processes (e.g. new outsourcing arrangements) and systems (e.g. IT change processes). In addition, The NPAP should ensure that approved products and changes are consistent with the risk strategy and risk appetite of the institution and the corresponding limits, or that necessary revisions are made.
148. Material changes or exceptional transactions may include mergers and acquisitions, including the potential		Material changes or exceptional transactions may include mergers and acquisitions, including the potential consequences of conducting insufficient due diligence

EBA Guidelines 2017	EBA Guidelines 2011	Differences
consequences of conducting insufficient due diligence that fails to identify post-merger risks and liabilities; setting up structures (e.g. new subsidiaries or single purpose vehicles; new products; changes to systems or the risk management framework or procedures; and changes to the institution's organisation.		that fails to identify post-merger risks and liabilities; setting up structures (e.g. new subsidiaries or single purpose vehicles; new products; changes to systems or the risk management framework or procedures; and changes to the institution's organisation.
149. An institution should have specific procedures for assessing compliance with these policies, taking into account the input of the risk management function. This should include a systematic prior assessment and documented opinion by the compliance function for new products or significant changes to existing products.		Under the new Guidelines, an institution should have specific procedures for assessing compliance with these policies, taking into account the input of the risk management function. This should include a systematic prior assessment and documented opinion by the compliance function for new products or significant changes to existing products.
150. An institution's NPAP should cover every consideration to be taken into account before deciding to enter new markets, deal in new products, launch a new service, or make significant changes to existing products or services. The NPAP should also include the definitions of 'new product/market/business' and 'significant changes' to be used in the organisation and the internal functions to be involved in the decision-making process.	2. 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' to be used in the organisation and the internal functions to be involved in the decision-making process.	Under the new Guidelines, the NPAP should also include an definition of 'significant changes' to be used in the organisation.
151. The NPAP should set out the main issues to be addressed before a decision is made. These should include regulatory compliance; accounting; pricing models; the impact on risk profile, capital adequacy and profitability; the availability of adequate front, back and middle office resources; and the availability of adequate internal tools and expertise to	3. The NPAP should set out the main issues to be addressed before a decision is made. These should include regulatory compliance, 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	No difference.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
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.	associated risks. The decision to launch a new activity should clearly state the business unit and individuals responsible for it. A new activity should not be undertaken until adequate resources to understand and manage the associated risks are available.	
152. The risk management function and the compliance function should be involved in approving new products or significant changes to existing products, processes and systems. Their input should include a full and objective assessment of risks arising from new activities under a variety of scenarios, of any potential shortcomings in the institution's risk	4. The Risk Control function should be involved in approving new products or significant changes to existing products. 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 Control function should also have a clear overview of the roll-out of new products (or significant changes to existing products) across different business lines and portfolios and the power to require that changes to existing products go through the formal NPAP process.	Under the new Guidelines both the risk management function and the compliance function should be involved in approving new products or significant changes to existing products, processes and systems, whereas under the old Guidelines only the Risk Control Function had to be involved in approving new products or significant changes to existing products
	D. Internal control	
19 Internal control functions	*24. Internal control framework*	
153. The internal control functions should include a risk management function (see Section 20), a compliance function (see Section 21) and an internal audit function (see Section 22). The risk management and compliance functions should be subject to review by the internal audit function.	1. An institution shall develop and maintain a strong and comprehensive internal control framework, including specific independent control functions with appropriate standing to fulfil their mission. (…) 4. An appropriate internal control framework also requires verification by independent	No material differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	control functions that these policies and procedures are complied with. The control functions should include a Risk Control function, a Compliance function and an Internal Audit function.	
154. The operational tasks of the internal control functions may be outsourced, taking into account the proportionality criteria listed in Title I, to the consolidating institution or another entity within or outside of the group with the consent of the management bodies of the institutions concerned. Even when internal control operational tasks are partially or fully outsourced, the head of the internal control function concerned and the management body are still responsible for these activities and for maintaining an internal control function within the institution.	2. The internal control framework of an institution should ensure effective and efficient operations, adequate control of risks, prudent conduct of business, reliability of financial and non-financial information reported, both internally and externally, and compliance with laws, regulations, supervisory requirements and the institution's internal rules and decisions. The internal control framework should cover the whole organisation, including the activities of all business, support and control units. The internal control framework should be appropriate for an institution's business, with sound administrative and accounting procedures.	Instead of a general provision on the internal control framework and the responsibility of this framework, different provisions entail requirements for the distinct functions of this internal control framework. Consequently, the more general formulated guideline has been repealed.
	3. In developing its internal control framework, an institution should ensure there is a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority to ensure compliance with internal rules and decisions. In order to implement a strong internal control framework in all areas of the institution, the business and support units should be responsible in the first place for establishing and maintaining adequate internal control policies and procedures.	
19.1 Heads of the internal control functions		

EBA Guidelines 2017	EBA Guidelines 2011	Differences
155. Heads of internal control functions should be established at an adequate hierarchical level that provides the head of the control function with the appropriate authority and stature needed to fulfil his or her responsibilities. Notwithstanding the overall responsibility of the management body, heads of internal control functions should be independent of the business lines or units they control. To this end, the heads of the risk management, compliance and internal audit functions should report and be directly accountable to the management body, and their performance should be reviewed by the management body.	5. The control functions should be established at an adequate hierarchical level and report directly to the management body. They should be independent of the business and support units they monitor and control as well as organisationally independent from each other (since they perform different functions). However, in less complex or smaller institutions, the tasks of the Risk Control and Compliance function may be combined. The group control functions should oversee the subsidiaries‟ control functions.	In the new Guidelines, it is specified that the heads of the risk management, compliance and internal audit functions should report and be directly accountable to the Executive and Supervisory Board, and their performance should be reviewed by these Boards.
156. Where necessary, the heads of internal control functions should be able to have access and report directly to the management body in its supervisory function to raise concerns and warn the supervisory function, where appropriate, when specific developments affect or may affect the institution. This should not prevent the heads of internal control functions from reporting within the regular reporting lines as well.	-	Under the new Guidelines, the heads of internal control functions should, where necessary, be able to have access and report directly to the Supervisory Board to raise concerns and warn the supervisory function, where appropriate, when specific developments affect or may affect the institution. This should not prevent the heads of internal control functions from reporting within the regular reporting lines as well.
157. Institutions should have documented processes in place to assign the position of the head of an internal control function and for withdrawing his or her responsibilities. In any case, the heads of internal control functions should – and under Article 76(5) of Directive 2013/36/EU the head of the risk management function must – not be removed without the prior approval of the management body in its	-	Institutions should have documented processes in place to assign the position of the head of an internal control function and for withdrawing his or her responsibilities. Under the new Guidelines, the heads of internal control functions, i.e. the risk management function, the internal audit function and the compliance function, should in any case not be removed without the prior approval of the management body in its supervisory function. Currently,

EBA Guidelines 2017	EBA Guidelines 2011	Differences
supervisory function. In significant institutions, competent authorities should be promptly informed about the approval and the main reasons for the removal of a head of an internal control function.		only the removal of the head of the risk management function requires prior approval of the Supervisory Board (Article 76(5) of CRD IV).
19.2 Independence of internal control functions		
158. In order for the internal control functions to be regarded as independent, the following conditions should be met: a. their staff do not perform any operational tasks that fall within the scope of the activities the internal control functions are intended to monitor and control; b. they are organisationally separate from the activities they are assigned to monitor and control; c. notwithstanding the overall responsibility of members of the management body for the institution, the head of an internal control function should not be subordinate to a person who has responsibility for managing the activities the internal control function monitors and controls; and d. the remuneration of the internal control functions' staff should not be linked to the performance of the activities the internal control function monitors and controls, and not otherwise likely to compromise their objectivity.	6. In order for the control function to be regarded as independent the following conditions should be met: a. its staff does not perform any tasks that fall within the scope of the activities the control function is intended to monitor and control; b. the control function is organisationally separate from the activities it is assigned to monitor and control; c. the head of the control function is subordinate to a person who has no responsibility for managing the activities the control function monitors and controls. The head of the control function generally should report directly to the management body and any relevant committees and should regularly attend their meetings; and d. the remuneration of the control function's staff should not be linked to the performance of the activities the control function monitors and controls, and not otherwise likely to compromise their objectivity.	No differences.
19.3 Combination of internal control functions		
159. Taking into account the proportionality criteria set out in Title I, the risk management function and compliance function may be		Under the new Guidelines, the risk management function and compliance function in the event the proportionality criteria can be applied to the concerned institution. The

EBA Guidelines 2017	EBA Guidelines 2011	Differences
combined. The internal audit function should not be combined with another internal control function.		internal audit function should, however, not be combined with another internal control function.
19.4 Resources of internal control functions		
160. Internal control functions should have sufficient resources. They should have an adequate number of qualified staff (both at parent level and at subsidiary level). Staff should remain qualified on an ongoing basis and should receive training as necessary.	7. Control functions should have an adequate number of qualified staff (both at parent and subsidiary level in groups). Staff should be qualified on an ongoing basis, and should receive proper training. (…)	Under the new Guidelines, the internal functions should have sufficient resources, next to an adequate number of qualified staff.
161. Internal control functions should have appropriate IT systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities. They should have access to all necessary information regarding all business lines and relevant risk-bearing subsidiaries, in particular those that can potentially generate material risks for the institutions.	7. (…) They should also have appropriate data systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities.	In the new Guidelines it is specified that (staff members of) the internal functions should have access to all necessary information regarding all business lines and relevant risk-bearing subsidiaries, in particular those that can potentially generate material risks for the institutions.
20 Risk management function	*25. Risk Control function (RCF)*	
162. Institutions should establish a risk management function (RMF) covering the whole institution. The RMF should have sufficient authority, stature and resources, taking into account the proportionality criteria listed in Title I, to implement risk policies and the risk management framework as set out in Section 17.	1. An institution shall establish a comprehensive and independent Risk Control function.	In the new Guidelines, it is specified that the risk management function (RMF) should have sufficient authority, stature and resources.
163. The RMF should have, where necessary, direct access to the management body in its supervisory function and its committees, where established, including in particular the risk committee.	-	The RMF should have, where necessary, direct access to the management body in its supervisory function and its committees, where established, including in particular the risk committee.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
164. The RMF should have access to all business lines and other internal units that have the potential to generate risk, as well as to relevant subsidiaries and affiliates.	-	The RMF should have access to all business lines and other internal units that have the potential to generate risk, as well as to relevant subsidiaries and affiliates.
165. Staff within the RMF should possess sufficient knowledge, skills and experience in relation to risk management techniques and procedures, and markets and products, and should have access to regular training.	-	Staff within the RMF should possess sufficient knowledge, skills and experience in relation to risk management techniques and procedures, and markets and products, and should have access to regular training.
166. The RMF should be independent of the business lines and units whose risks it controls but should not be prevented from interacting with them. Interaction between the operational functions and the RMF should help to achieve the objective of all the institution's staff bearing responsibility for managing risk.	4. The RCF should be independent of the business and support units whose risks it controls but not be isolated from them. It should possess sufficient knowledge on risk management techniques and procedures and on markets and products. Interaction between the operational functions and the RCF should facilitate the objective that all the institution's staff bears responsibility for managing risk.	No differences.
167. The RMF should be a central organisational feature of the institution, structured so that it can implement risk policies and control the risk management framework. The RMF should play a key role in ensuring that the institution has effective risk management processes in place. The RMF should be actively involved in all material risk management decisions.	3. The RCF should be an institution's central organisational feature, structured so it can implement risk policies and control the risk management framework. Large, complex and sophisticated institutions may consider establishing dedicated RCFs for each material business line. However, there should be in the institution a central RCF (including where appropriate a Group RCF in the parent company of a group) to deliver a holistic view on all the risks	In the new Guidelines, it is specified that the RMF should be actively involved in all material risk management decisions.
168. Significant institutions may consider establishing dedicated RMFs for each material business line. However, there should be a central RMF, including a group RMF in the		Significant institutions may consider establishing dedicated RMFs for each material business line. However, there should be a central RMF, including a group RMF in the consolidating institution, to deliver an

EBA Guidelines 2017	EBA Guidelines 2011	Differences
consolidating institution, to deliver an institution- and group-wide holistic view on all risks and to ensure that the risk strategy is complied with.		institution- and group-wide holistic view on all risks and to ensure that the risk strategy is complied with
169. The RMF should provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by business lines or internal units, and should inform the management body as to whether they are consistent with the institution's risk appetite and strategy. The RMF may recommend improvements to the risk management framework and corrective measures to remedy breaches of risk policies, procedures and limits.	2. The RCF should ensure each key risk the institution faces is identified and properly managed by the relevant units in the institution and a holistic view on all relevant risks is submitted to the management body. The RCF should provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by the management body and business or support units as to whether they are consistent with the institution's risk tolerance/appetite. The RCF may recommend improvements to the risk management framework and options to remedy breaches of risk policies, procedures and limits	No material differences.
20.1 RMF's role in risk strategy and decisions	*26. The Risk Control Function's role*	
170. The RMF should be actively involved at an early stage in elaborating an institution's risk strategy and in ensuring that the institution has effective risk management processes in place. The RMF should provide the management body with all relevant risk-related information to enable it to set the institution's risk appetite level. The RMF should assess the robustness and sustainability of the risk strategy and appetite. It should ensure that the risk appetite is appropriately translated into specific risk limits. The RMF should also assess the risk strategies of business units,	1. The RCF shall be actively involved at an early stage in elaborating an institution's risk strategy and in all material risk management decisions. The RCF shall play a key role in ensuring the institution has effective risk management processes in place. 2. The RCF should provide the management body with all relevant risk related information (e.g. through technical analysis on risk exposure) to enable it to set the institution's risk tolerance/appetite level.	Guideline 26.4 has been repealed.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
including targets proposed by the business units, and should be involved before a decision is made by the management body concerning the risk strategies. Targets should be plausible and consistent with the institutions risk strategy.	3. The RCF should also assess the risk strategy, including targets proposed by the business units, and advise the management body before a decision is made. Targets, which include credit ratings and rates of return on equity, should be plausible and consistent. 4. The RCF should share responsibility for implementing an institution's risk strategy and policy with all the institution's business units. While the business units should implement the relevant risk limits, the RCF should be responsible for ensuring the limits are in line with the institution's overall risk appetite/risk tolerance and monitoring on an on-going basis that the institution is not taking on excessive risk.	
171. The RMF's involvement in decision-making processes should ensure that risk considerations are taken into account appropriately. However, accountability for the decisions taken should remain with the business and internal units, and ultimately the management body.	5. The RCF"s involvement in the decision-making processes should ensure risk considerations are taken into account appropriately. However, accountability for the decisions taken should remain with the business and support units and ultimately the management body.	No differences.
20.2 RMF's role in material changes		
172. In line with Section 18, before decisions on material changes or exceptional transactions are taken, the RMF should be involved in the evaluation of the impact of such changes and exceptional transactions on the institution's and group's overall risk, and should report its findings directly to the management body before a decision is taken.	9. Before decisions on material changes or exceptional transactions are taken, the RCF should be involved in the evaluation of the impact of such changes and exceptional transactions.	Under the new Guidelines, RMF should report its findings concerning the impact of material changes or exceptional transactions on the institution's and group's overall risk directly to the management body before a decision is taken.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
173. The RMF should evaluate how risks identified could affect the institution's or group's ability to manage its risk profile, its liquidity and its sound capital base under normal and adverse circumstances.	8. The RCF should evaluate how any material risks identified could affect the institution or group's ability to manage its risk profile and deploy funding and capital under normal and adverse circumstances.	No differences.
20.3 RMF's role in identifying, measuring, assessing, managing, mitigating, monitoring and reporting on risks		
174. The RMF should ensure that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the institution.		Under the new Guidelines, the RMF has an explicit responsibility to ensure that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the institution.
175. The RMF should ensure that identification and assessment are not based only on quantitative information or model outputs, and take into account also qualitative approaches. The RMF should keep the management body informed of the assumptions used in and potential shortcomings of the risk models and analysis.	10.The RCF should ensure that an institution's internal risk measurements and assessments cover an appropriate range of scenarios and are based on sufficiently conservative assumptions regarding dependencies and correlations. This should include qualitative (including with expert judgement) firm-wide views on the relationships between the risks and profitability of the institution and its external operating environment.	No differences.
176. The RMF should ensure that transactions with related parties are reviewed and that the risks they pose for the institution are identified and adequately assessed.	6. The RCF should ensure transactions with related parties are reviewed and the risks, actual or potential, they pose for the institution are identified and adequately assessed.	No differences.
177. The RMF should ensure that all identified risks are effectively monitored by the business units.	11.The RCF should ensure all identified risks can be effectively monitored by the business units. (…)	No differences.
178. The RMF should regularly monitor the actual risk profile of the institution and scrutinise it against the institution's strategic	11. (…) The RCF should regularly monitor the actual risk profile of the institution and scrutinise it against the institution's strategic	No differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
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.	goals, risk tolerance/appetite to enable decision making by the management body in its management function and challenge by the management body in its supervisory function.	
179. The RMF should analyse trends and recognise new or emerging risks and risk increases arising from changing circumstances and conditions. It should also regularly review actual risk outcomes against previous estimates (i.e. back testing) to assess and improve the accuracy and effectiveness of the risk management process.	12.The RCF should analyse trends and recognise new or emerging risks 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.	No differences.
180. The RMF should evaluate possible ways to mitigate risks. Reporting to the management body should include proposed appropriate risk-mitigating actions.		Under the new Guidelines, the RMF has the responsibility to evaluate possible ways to mitigate risks. Reporting to the management body should include proposed appropriate risk-mitigating actions.
-	13.The group RCF should monitor the risks taken by the subsidiaries. Inconsistencies with the approved group strategy should be reported to the relevant management body.	
20.4 RMF's role in unapproved exposures	*RCF's role in unapproved exposures*	
181. The RMF should independently assess breaches of risk appetite or limits (including ascertaining the cause and undertaking a legal and economic analysis of the actual cost of closing, reducing or hedging the exposure against the potential cost of keeping it). The RMF should inform the business units concerned and the management body, and recommend possible remedies. The RMF should report directly to the management body in its supervisory function when the breach is	14.The RCF should be adequately involved in any changes to the institution's strategy, approved risk tolerance/appetite and limits. 15.The RCF should independently assess a breach or violation (including its 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 RCF should inform, as appropriate, the business units concerned and recommend possible	Under the new Guidelines, the RMF should report directly to the management body in its supervisory function when a breach of risk appetite or limits is material, without prejudice for the RMF to report to other internal functions and committees.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
material, without prejudice for the RMF to report to other internal functions and committees.	remedies.	
182. The RMF should play a key role in ensuring a decision on its recommendation is made at the relevant level, complied with by the relevant business units and appropriately reported to the management body and, where established, the risk committee.	16. The RCF 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, risk committee and business or support unit.	No differences.
	17. An institution should take appropriate actions against internal or external fraudulent behaviour and breaches of discipline (e.g. breach of internal procedures, breach of limits).	This old Guideline has been implemented in Guideline 195 of the new Guidelines.
20.5 Head of the risk management function	*27. Chief Risk Officer*	
183. The head of the RMF should be responsible for providing comprehensive and understandable information on risks and advising the management body, enabling this body to understand the institution's overall risk profile. The same applies to the head of the RMF of a parent institution regarding the consolidated situation.	1. An institution shall appoint a person, the Chief Risk Officer ('CRO'), with exclusive responsibility for the RCF and for monitoring the institution's risk management framework across the entire organisation. 2. The CRO (or equivalent position) shall 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 CRO of a parent institution regarding the whole group.	No material differences. The head of the RMF equals the CRO under the old Guidelines.
184. The head of the RMF should have sufficient expertise, independence and seniority to challenge decisions that affect an institution's exposure to risks. When the head of the RMF is not a member of the management body, significant institutions	3. The CRO should have sufficient expertise, operating experience, independence and seniority to challenge decisions that affect an institution's exposure to risk. (…) 5. When an institution's characteristics –	The new Guidelines specify that in the event the head of the RMF is not a member of the management body, significant institutions should appoint an independent head of the RMF who has no responsibilities for other functions and reports directly to the management body.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
should appoint an independent head of the RMF who has no responsibilities for other functions and reports directly to the management body. Where it is not proportionate to appoint a person who is dedicated only to the role of head of the RMF, taking into account the principle of proportionality as set out in Title I, this function can be combined with the head of the compliance function or can be performed by another senior person, provided there is no conflict of interest between the functions combined. In any case, this person should have sufficient authority, stature and independence (e.g. head of legal).	notably its size, organisation and the nature of its activities – do not justify entrusting such responsibility to a specially appointed person, the function could be fulfilled by another senior person within the institution, provided there is no conflict of interest.	
185. The head of the RMF should be able to challenge decisions taken by the institution's management and its management body, and the grounds for objections should be formally documented. If an institution wishes to grant the head of the RMF the right to veto decisions (e.g. a credit or investment decision or the setting of a limit) made at levels below the management body, it should specify the scope of such a veto right, the escalation or appeal procedures, and how the management body will be involved.	3. (…) An institution should consider granting a veto right to the CRO. The CRO and the management body or relevant committees should be able to communicate directly among themselves on key risk issues including developments that may be inconsistent with the institution's risk tolerance/appetite and strategy. 4. If an institution wishes to grant the CRO the right to veto decisions, its risk policies should set out the circumstances the CRO may do this and the nature of the proposals (e.g. a credit or investment decision or the setting of a limit). The policies should describe the escalation or appeals procedures and how the management body is informed.	No material differences.
	6. The institution should have documented processes in place to assign the position of the	Under the new Guidelines, the heads of internal control functions, i.e. the risk management function, the internal

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	CRO and to withdraw his or her responsibilities. If the CRO is replaced it should be done with the prior approval of the management body in its supervisory function. Generally the removal or appointment of a CRO should be disclosed and the supervisory authority informed about the reasons.	audit function and the compliance function, should in any case not be removed without the prior approval of the management body in its supervisory function. Currently, only the removal of the head of the risk management function requires prior approval of the Supervisory Board (Article 76(5) of CRD IV).
186. Institutions should establish strengthened processes for the approval of decisions on which the head of the RMF has expressed a negative view. The management body in its supervisory function should be able to communicate directly with the head of the RMF on key risk issues, including developments that may be inconsistent with the institution's risk appetite and strategy.		Under the new Guidelines, institutions should establish strengthened processes for the approval of decisions on which the head of the RMF has expressed a negative view. The management body in its supervisory function should be able to communicate directly with the head of the RMF on key risk issues, including developments that may be inconsistent with the institution's risk appetite and strategy.
21 Compliance function	*28. Compliance function*	
187. Institutions should establish a permanent and effective compliance function to manage compliance risk and should appoint a person to be responsible for this function across the entire institution (the compliance officer or head of compliance).	1. An institution shall establish a Compliance function to manage its compliance risk. 3. An institution should establish a permanent and effective Compliance function and appoint a person responsible for this function across the entire institution and group (the Compliance Officer or Head of Compliance). (…)	
188. Where it is not proportionate to appoint a person who is dedicated only to the role of head of compliance, taking into account the principle of proportionality as set out in Title I, this function can be combined with the head of the RMF or can be performed by another senior person (e.g. head of legal), provided there is no conflict of interest between the functions	3. (…) In smaller and less complex institutions this function may be combined with or assisted by the risk control or support functions (e.g. HR, legal, etc).	No material differences, although is under the new Guidelines it is explicitly specified that the role of head of compliance can be combined with other functions, provided that there is no conflict of interest between the functions combined.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
combined		
189. The compliance function, including the head of compliance, should be independent of the business lines and internal units it controls and have sufficient authority, stature and resources. Taking into account the proportionality criteria set out in Title I, this function may be assisted by the RMF or combined with the RMF or other appropriate functions, e.g. the legal division or human resources		The compliance function, including the head of compliance, should under the new Guidelines be independent of the business lines and internal units it controls and have sufficient authority, stature and resources. Taking into account the proportionality criteria set out in Title I, this function may be assisted by the RMF or combined with the RMF or other appropriate functions, e.g. the legal division or human resources
190. Staff within the compliance function should possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures, and should have access to regular training.		Staff within the compliance function should possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures, and should have access to regular training.
191. The management body in its supervisory function should oversee the implementation of a well-documented compliance policy, which should be communicated to all staff. Institutions should set up a process to regularly assess changes in the law and regulations applicable to its activities.	2. An institution shall approve and implement a compliance policy which should be communicated to all staff.	Under the new Guidelines, the Supervisory Board has an explicit obligation to oversee the implementation of a well-documented compliance policy, which should be communicated to all staff. Institutions should set up a process to regularly assess changes in the law and regulations applicable to its activities. Under the old Guidelines, the institution had the obligation to approve and implement a compliance policy which should be communicated to all staff. Under the new Guidelines, this responsibility is assigned to the management function in its supervisory function.
192. The compliance function should advise the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and should assess the possible impact of any changes in	5. The Compliance function should advise the management body on laws, rules, regulations and standards the institution needs to meet and assess the possible impact of any changes in the legal or regulatory environment on the	No differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
the legal or regulatory environment on the institution's activities and compliance framework.	institution's activities.	
193. The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that the compliance policy is observed. The compliance function should report to the management body and communicate as appropriate with the RMF on the institution's compliance risk and its management. The compliance function and the RMF should cooperate and exchange information as appropriate to perform their respective tasks. The findings of the compliance function should be taken into account by the management body and the RMF in decision-making processes.	4. The Compliance function should ensure that the compliance policy is observed and report to the management body and as appropriate to the RCF on the institution's management of compliance risk. The findings of the Compliance function should be taken into account by the management body and the RCF within the decision-making process	Under the new Guidelines, it is made explicit that the compliance function and the RMF should cooperate and exchange information as appropriate to perform their respective tasks..
194. In line with Section 18 of these guidelines, the compliance function should also verify, in close cooperation with the RMF and the legal unit, that new products and new procedures comply with the current legal framework and, where appropriate, with any known forthcoming changes to legislation, regulations and supervisory requirements.	6. The Compliance function should also verify that new products and new procedures comply with the current legal environment and any known forthcoming changes to legislation, regulations and supervisory requirements.	Here again, the close cooperation of the compliance function with the RMF and the legal unit is reiterated.
195. Institutions should take appropriate action against internal or external fraudulent behaviour and breaches of discipline (e.g. breaches of internal procedures, breaches of limits).	26.17. An institution should take appropriate actions against internal or external fraudulent behaviour and breaches of discipline (e.g. breach of internal procedures, breach of limits).	
196. Institutions should ensure that their subsidiaries and branches take steps to ensure		Under the new Guidelines, institutions should ensure that their subsidiaries and branches take steps to ensure that

EBA Guidelines 2017	EBA Guidelines 2011	Differences
that their operations are compliant with local laws and regulations. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches should inform the compliance officer or the head of compliance of the consolidating institution.		their operations are compliant with local laws and regulations. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches should inform the compliance officer or the head of compliance of the consolidating institution.
22 Internal audit function	*29. Internal Audit function*	
197. Institutions should set up an independent and effective internal audit function (IAF), taking into account the proportionality criteria set out in Title I, and should appoint a person to be responsible for this function across the entire institution. The IAF should be independent and have sufficient authority, stature and resources. In particular, the institution should ensure that the qualification of the IAF's staff members and the IAF's resources, in particular its auditing tools and risk analysis methods, are adequate for the institution's size and locations, and the nature, scale and complexity of the risks associated with the institution's business model, activities, risk culture and risk appetite.	1. The Internal Audit function ('IAF') shall assess whether the quality of an institution's internal control framework is both effective and efficient.	The new Guidelines specify the requirements regarding the internal audit function (IAF). The institutions should appoint a person to be responsible for this function across the entire institution. The IAF should be independent and have sufficient authority, stature and resources. In particular, the institution should ensure that the qualification of the IAF's staff members and the IAF's resources, in particular its auditing tools and risk analysis methods, are adequate for the institution's size and locations, and the nature, scale and complexity of the risks associated with the institution's business model, activities, risk culture and risk appetite.
198. The IAF should be independent of the audited activities. Therefore, the IAF should not be combined with other functions.	3. The IAF should evaluate the compliance of all activities and units of an institution (including the RCF and Compliance function) with its policies and procedures. Therefore, the IAF should not be combined with any other function. The IAF should also assess whether	No material differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	existing policies and procedures remain adequate and comply with legal and regulatory requirements	
199. The IAF should, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of an institution, including outsourced activities, with the institution's policies and procedures and with external requirements. Each entity within the group should fall within the scope of the IAF.	3. The IAF should evaluate the compliance of all activities and units of an institution (including the RCF and Compliance function) with its policies and procedures. Therefore, the IAF should not be combined with any other function. The IAF should also assess whether existing policies and procedures remain adequate and comply with legal and regulatory requirements	No material differences, although the new Guideline explicitly mentions that the review of the AIF should follow a risk-based approach and that the review should also cover the outsourced activities.
200. The IAF should not be involved in designing, selecting, establishing and implementing specific internal control policies, mechanisms and procedures, and risk limits. However, this should not prevent the management body in its management function from requesting input from internal audit on matters related to risk, internal controls and compliance with applicable rules.	4. (…) However, in order to strengthen its independence, the IAF should not be directly involved in the design or selection of models or other risk management tools.	Under the new Guidelines, it is made explicit that the Executive Board should not refrain from requesting input from internal audit on matters related to risk, internal controls and compliance with applicable rules in order to preserve the independence of the IAF.
201. The IAF should assess whether the institution's internal control framework as set out in Section 15 is both effective and efficient. In particular, the IAF should assess: a. the appropriateness of the institution's governance framework; b. whether existing policies and procedures remain adequate and comply with legal and regulatory requirements and with the risk appetite and strategy of the institution; c. the compliance of the procedures with the		In the new Guidelines, it is specified which elements of the institution's internal control framework, the AIF should assess in its review of the functioning of this framework.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
applicable laws and regulations and with decisions of the management body; d. whether the procedures are correctly and effectively implemented (e.g. compliance of transactions, the level of risk effectively incurred, etc.); and e. the adequacy, quality and effectiveness of the controls performed and the reporting done by the defence business units and the risk management and compliance functions.		
202. The IAF should verify, in particular, the integrity of the processes ensuring the reliability of the institution's methods and techniques, and the assumptions and sources of information used in its internal models (e.g. risk modelling and accounting measurements). It should also evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken.	4. 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. (…)	
203. The IAF should have unfettered institution-wide access to all the records, documents, information and buildings of the institution. This should include access to management information systems and minutes of all committees and decision-making bodies.	2. The IAF should have unfettered access to relevant documents and information in all operational and control units.	In the new Guidelines, it is further specified what unfettered institution-wide access to all the records, documents, information and buildings of the institution entails.
204. The IAF should adhere to national and international professional standards. An example of the professional standards referred to here is the standards established by the Institute of Internal Auditors.	5. The management body should encourage the internal auditors to adhere to national and international professional standards. (…)	No material differences. The New Guideline refers to a specific example of professional standards.
205. Internal audit work should be performed in accordance with an audit plan and a detailed audit programme following a risk-based	5. (…) Internal audit work should be performed in accordance with an audit plan and detailed audit programs following a 'risk based'	No differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
approach.	approach. (…)	
206. An internal audit plan should be drawn up at least once a year on the basis of the annual internal audit control objectives. The internal audit plan should be approved by the management body.	5. (…) The audit plan should be approved by the audit committee and/or the management body.	Under the new Guidelines, an internal audit plan should be drawn up at least once a year on the basis of the annual internal audit control objectives.
207. All audit recommendations should be subject to a formal follow-up procedure by the appropriate levels of management to ensure and report on their effective and timely resolution.	6. The IAF should report directly to the management body and/or its audit committee (where applicable) its findings and suggestions for material improvements to internal controls. All audit recommendations should be subject to a formal follow-up procedure by the respective levels of management to ensure and report their resolution.	No differences.
Title VI – Business continuity management	***E. Information systems and business continuity***	
	30. Information system and communication	
	1. An institution shall have effective and reliable information and communication systems covering all its significant activities.	Under the new Guidelines, an institution shall have effective and reliable information and communication systems covering all its significant activities.
	2. Information systems, including those that hold and use data in electronic form, should be secure, independently monitored and supported by adequate contingency arrangements. An institution should comply with generally accepted IT Standards when implementing IT systems.	Information systems, including those that hold and use data in electronic form, should be secure, independently monitored and supported by adequate contingency arrangements. An institution should comply with generally accepted IT Standards when implementing IT systems.
	31. Business continuity management	
208. Institutions should establish a sound business continuity management plan to ensure their ability to operate on an ongoing basis and to limit losses in the event of severe business disruption.	1. An institution shall 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.	No differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
209. Institutions may establish a specific independent business continuity function, e.g. as part of the RMF.		Under the new Guidelines, institutions may establish a specific independent business continuity function, e.g. as part of the RMF. See also Article 312 of Regulation (EU) No 575/2013.
210. An institution's business relies on several critical resources (e.g. IT systems including cloud services, communication systems and buildings). The purpose of business continuity management is to reduce the operational, financial, legal, reputational and other material consequences arising from a disaster or extended interruption to these resources and consequent disruption to the institution's ordinary business procedures. Other risk management measures might be intended to reduce the probability of such incidents or to transfer their financial impact to third parties (e.g. through insurance).		In the new Guidelines, the purpose of business continuity management is defined.
211. In order to establish a sound business continuity management plan, an institution should carefully analyse its exposure to severe business disruptions and assess (quantitatively and qualitatively) their potential impact, using internal and/or external data and scenario analysis. This analysis should cover all business lines and internal units, including the RMF, and should take into account their interdependency. The results of the analysis should contribute to defining the institution's recovery priorities and objectives.	2. 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 and support units and the RCF and take into account their interdependency. In addition, a specific independent Business Continuity function, the RCF or the Operational Risk Management function should be actively involved. The results of the analysis should contribute to define the institutions‟ recovery	No differences.

EBA Guidelines 2017	EBA Guidelines 2011	Differences
	priorities and objectives.	
212. On the basis of the abovementioned analysis, an institution should put in place: a. contingency and business continuity plans to ensure that the institution reacts appropriately to emergencies and is able to maintain its most important business activities if there is disruption to its ordinary business procedures; and b. recovery plans for critical resources to enable the institution to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions should be consistent with the institution's risk appetite.	3. 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. 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 tolerance/appetite.	No differences
213. Contingency, business continuity and recovery plans should be documented and carefully implemented. The documentation should be available within the business lines, internal units and RMF, and should be stored on systems that are physically separated and readily accessible in case of contingency. Appropriate training should be provided. Plans should be regularly tested and updated. Any challenges or failures occurring in the tests should be documented and analysed, with the plans reviewed accordingly.	4. Contingency, business continuity and recovery plans should be documented and carefully implemented. The documentation should be available within the business, support units and the RCF, 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.	No differences
Title VII – Transparency	***F. Transparency***	
	32. Empowerment	
214. Strategies, policies and procedures should be communicated to all relevant staff throughout an institution. An institution's staff should understand and adhere to policies and	1. Strategies and policies shall be communicated to all relevant staff throughout an institution.	No differences

EBA Guidelines 2017	EBA Guidelines 2011	Differences
procedures pertaining to their duties and responsibilities.	2. An institution's staff should understand and adhere to policies and procedures pertaining to their duties and responsibilities.	
215. Accordingly, the management body should inform and update the relevant staff about the institution's strategies and policies in a clear and consistent way, at least to the level needed to carry out their particular duties. This may be done through written guidelines, manuals or other means.	3. 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.	No differences
	33. Internal governance transparency	
216. Where parent undertakings are required by competent authorities under Article 106(2) of Directive 2013/36/EU to publish annually a description of their legal structure and governance and the organisational structure of the group of institutions, the information should include all entities within the group structure as defined in Directive 2013/34/EU, by country.	1. The internal governance framework of an institution shall be transparent. An institution shall present its current position and future prospects in a clear, balanced, accurate and timely way.	In the event parent undertakings are required by competent authorities under Article 106(2) of Directive 2013/36/EU to publish annually a description of their legal structure and governance and the organisational structure of the group of institutions, the information should include all entities within the group structure as defined in Directive 2013/34/EU, by country.
217. The publication should include at least: a. an overview of the internal organisation of the institutions and the group structure as defined in Directive 2013/34/EU and changes thereto, including the main reporting lines and responsibilities; b. any material changes since the previous publication and the date of the material change; c. new legal, governance or organisational structures; d. information on the structure, organisation and members of the management body,	2. An institution should publicly disclose at least the following: a. its governance structures and policies, including its objectives, organisational structure, internal governance arrangements, structure and organisation of the management body, including attendances, and the incentive and remuneration structure of the institution; b. the nature, extent, purpose and economic substance of transactions with affiliates and related parties, if they have a material impact on the institution; c. how its business and risk	The publication should under the new Guidelines include at least: a. an overview of the internal organisation of the institutions and the group structure as defined in Directive 2013/34/EU and changes thereto, including the main reporting lines and responsibilities; b. any material changes since the previous publication and the date of the material change; c. new legal, governance or organisational structures; d. information on the structure, organisation and members of the management body, including the number of its members and the number of those qualified as

EBA Guidelines 2017	EBA Guidelines 2011	Differences
including the number of its members and the number of those qualified as independent, and specifying the gender and duration of the mandate of each member of the management body; e. the key responsibilities of the management body; f. a list of the committees of the management body in its supervisory function and their composition; g. an overview of the conflict of interest policy applicable to the institutions and to the management body; h. an overview of the internal control framework; and i. an overview of the business continuity management framework.	strategy is set (including the involvement of the management body) and foreseeable risk factors; d. its established committees and their mandates and composition; e. its internal control framework and how its control functions are organised, the major tasks they perform, how their performance is monitored by the management body and any planned material changes to these functions; and f. material information about its financial and operating results.	independent, and specifying the gender and duration of the mandate of each member of the management body; e. the key responsibilities of the management body; f. a list of the committees of the management body in its supervisory function and their composition; g. an overview of the conflict of interest policy applicable to the institutions and to the management body; h. an overview of the internal control framework; and i. an overview of the business continuity management framework.
	3. Information about the current position of the institution should comply with any legal disclosure requirements. Information should be clear, accurate, relevant, timely and accessible.	
	4. In cases where ensuring a high degree of accuracy would delay the release of time-sensitive information, an institution should make a judgement as to the appropriate balance between timeliness and accuracy, bearing in mind the requirement to provide a true and fair picture of its situation and give a satisfactory explanation for any delay. This explanation should not be used to delay regular reporting requirements.	