27 September 2011

EBA Guidelines on Internal Governance

(GL 44)

Contents

I. Executive Summary 3

II. Background and rationale 7

1. Importance of internal governance 7

2. Purpose and scope of the Guidelines on Internal Governance 8

3. Concepts used in the Guidelines 9

III. EBA Guidelines on Internal Governance 12

Title I -Subject matter, Scope and definitions 16

Title II – Requirements regarding institutions' internal governance 16

Title III – Final Provisions and Implementation 48

IV. Accompanying documents 49

Cost and benefit analysis regarding the Internal Governance Guidelines 49

Feedback statement on the public consultation of the Guidelines on Internal Governance (CP 44) and on the opinion of the Banking Stakeholder Group 55

I. Executive Summary

1. **Internal governance** for institutions[1] in the European Community is covered by **Article 22 of Directive 2006/48/EC,** which requires 'that every credit institution has robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, adequate internal control mechanisms, including sound administrative and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management'. Article 73(3) of Directive 2006/48/EC requires that Article 22 also applies to parent undertakings and subsidiaries on a consolidated or sub-consolidated basis.

2. Trust in the reliability of the banking system is crucial for its proper functioning and a prerequisite if it is to contribute to the economy as a whole. Consequently, effective internal governance arrangements are fundamental if institutions, individually, and the banking system, are to operate well. It is on the basis of this understanding and within the above-mentioned framework that the Committee of European Banking Supervisors (CEBS) had issued guidelines covering either wholly or partially internal governance aspects: the 2006 Guidelines on Outsourcing; the 2006 Guidelines on Supervisory Review Process; the 2009 High Level Principles on Remuneration; the 2010 High Level Principles on Risk Management).

3. As a follow up to the financial crisis which erupted in 2008, CEBS conducted a survey on the implementation of internal governance by institutions and competent authorities. Weak internal governance issues were not identified as a direct trigger for the financial crisis, but rather as a crucial underlying factor. Weaknesses were often the result of an insufficient implementation of existing guidelines.

4. In order to take into account weaknesses identified in the financial crisis and developments since the publication of the former CEBS Guidelines (such as the updated Basel Committee for Banking Supervision- BCBS- guidance on 'Enhancing corporate governance for banking organisations'), the EBA updated

[1] Institutions referred to in these guidelines are credit institutions and investment firms as per Article 22 of the Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast) applies; for investment firms see also Article 34 of Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast), hereafter both directives are referred to as the Capital Requirements Directive (CRD). .

the former CEBS guidelines, on internal governance, and sought to consolidate them in these Internal Governance Guidelines, with references, where appropriate, to other guidelines covering more specific aspects of internal governance issues (such as outsourcing or remuneration). More in particular, the sections of the Guidelines on the Supervisory Review Process[2] that relate to internal governance have now been reviewed and merged with the High Level Principles on Remuneration and on Risk Management. New chapters on 'Risk Management' and 'Systems and Continuity' have been added.

5. In the first chapter on 'Corporate Structure and Organisation', the concept of checks and balances in group structures is discussed in more detail and the 'Know-your-structure' principle is introduced to remedy the weaknesses identified within the survey regarding complex structures which have not been understood and counterbalanced sufficiently. The aim of this part of the Guidelines is to limit opaque activities using non supervised structures.

6. The second chapter on 'Management Body' was enhanced by adding guidelines on the composition, appointment and succession and the qualifications of the management body, which focus more on the use of committees and the identification and management of conflicts of interest. As lack of oversight was one of the most significant weaknesses identified in the financial crisis, the aim of this part of the guidelines is to ensure that members of the management body (especially in its supervisory function) devote sufficient time to their functions. Finally, the responsibilities of the management body regarding outsourcing and setting the remuneration policy have also been added to the Guidelines, for completeness of the overview of the Management Body functions. Nevertheless, as separate CEBS guidelines exist regarding these aspects of internal governance, which are still applicable, references to them have been added to the text, as appropriate.[3]

7. The third chapter on 'Risk Management' took on board large parts of the High Level Principles on Risk Management (such as the high level principles on 'governance and risk culture', 'risk models and integration of risk management areas', 'new product approval policy and process'). Parts of the former high level principles on 'risk appetite and risk tolerance' have been assigned to the new guidelines on the risk management framework.

8. The fourth chapter on 'Internal Control' includes the section entitled 'The role of Chief Risk Officer and the risk management function' stemming from the High Level Principles on Risk Management and is aimed at ensuring the proper staffing of the control function, as one weakness identified in the CEBS survey mentioned above was that the control functions were not given

[2] The Guidelines on the Supervisory Review Process are available on the EBA website.
[3] The Guidelines are published on the EBA website.

sufficient resources to fulfil their duties. The principles also deal with the issue of unapproved exposures, aimed at implementing adequate processes for monitoring the set limits and taking appropriate actions where necessary.

9. The fifth chapter on 'Systems and Continuity' contains new guidelines on information and communication systems and business continuity management. Instead of formulating extensive requirements with regard to IT systems, the guidelines refer to generally accepted standards in this matter. The principles on business continuity are consistent with the BCBS 'High Level Principles for Business Continuity'.

10. The sixth chapter on 'Transparency' contains the chapter entitled 'Public Disclosure and Transparency' from the former CEBS Internal Governance Guidelines. Here, only limited amendments have been made to the previous version of the guidelines, as the CEBS survey did not identify major weaknesses in this area.

11. When developing these Guidelines, the EBA took into account the feedback received from stakeholders during the public consultation. EBA also assessed the costs and benefits of its proposals. The feedback statement from the public consultation and the cost-benefit analysis are attached as accompanying documents of these Guidelines.

12. Overall, the respondents have been supportive of the proposed Guidelines and appreciate the fact that the EBA has developed a comprehensive set of internal governance guidelines which is in line with international standards. The respondents also welcomed the application of the principle of proportionality. The respondents stated that the key issue during the financial crisis was not a lack of governance rules but a lack of effective implementation of these rules. A fully functioning and trusted banking system, supported by sound governance frameworks in institutions, is a key component in any modern economy.

13. On 27 May 2011 the draft Guidelines on Internal Governance were presented to the EBA's Banking Stakeholder Group (BSG). No formal opinion of the BSG was deemed necessary, given that the work started under the CEBS and the public had already been consulted about the Guidelines.

14. A cost and benefit analysis was also conducted, which used as its benchmark current legislation, in particular Directives 2006/48/EC and 2006/49/EC, which it compares against the changes effected by these Guidelines to the former CEBS Guidelines. In so doing, it also uses the results of the public consultation.

15. The cost and benefit analysis concluded, in relation to costs, that the implementation of the Guidelines will trigger moderate one-off costs in institutions and competent authorities, while the ongoing costs for an

improved governance framework and its supervision should be relatively low. In terms of benefits, the analysis suggested that institutions will benefit from an improved governance framework by a better alignment of their risk profile with their risk strategy/appetite and a better management of risks, which may lead to a reduction of losses. The implementation of the Guidelines is expected to result in a more resilient banking system. Therefore it was deemed that the benefits of introducing these revised guidelines considerably outweigh the costs that might be incurred by their introduction.

II. Background and rationale

1. Importance of internal governance

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

17. In recent years, internal governance issues have received the increasing attention of various international bodies[4]. Their main effort has been to correct the institutions' weak or superficial internal governance practices as identified in the financial crisis. These faulty practices, while not a direct trigger for the financial crisis, were closely associated with it and so were a key contributory factor.

18. The European Banking Authority (EBA) came into being on 1 January 2011 and has taken over all the existing and ongoing tasks and responsibilities of the Committee of European Banking Supervisors (CEBS). In late 2009, the CEBS undertook a **survey on the implementation** by supervisory authorities and institutions **of its Internal Governance Guidelines** published in January 2006[5]. The survey's main results[6] were that, although overall the regulatory and supervisory national frameworks for internal governance could be considered as largely complete, their coverage was somewhat fragmented and a number of gaps were identified. The survey also revealed that many institutions needed to improve their implementation of the Guidelines and supervisors needed to enhance their procedures in this respect.

19. With regard to corporate structure and organisation, the main weakness identified was that the institutions' **complexity** was not sufficiently

---

[4] See in particular:
BCBS 'Principles for enhancing corporate governance' of 4 October 2010 available at: http://www.bis.org/publ/bcbs176.htm ;
OECD 'Corporate governance and the financial crisis -Conclusions and emerging good practices to enhance implementation of the Principles' of February 2010 available at http://www.oecd.org/dataoecd/53/62/44679170.pdf ;
European Commission 'Green Paper on Corporate governance in financial institutions and remuneration policies' of June 2010, available at http://ec.europa.eu/internal_market/company/docs/modern/com2010_284_en.pdf .

[5] These are included in the 2006 CEBS Guidelines on the Application of the Supervisory Review Process under Pillar 2 to be found in the EBA website.

[6] A summary of the results can be seen at the EBA website under the following link: http://www.eba.europa.eu/documents/About-us/Key-dates/Summary-of-survey-results_Workshop-on-Internal-Gov.aspx.

counterbalanced by appropriate internal governance arrangements. The complexity and riskiness of the products and services offered by institutions and the different nature of local markets in which cross-border groups operate, compounded the level of the institutions' complexity. The corporate structure was neither always transparent nor organised in a way that promoted and demonstrated effective and prudent management, often because of ineffective reporting lines.

20. Weak **oversight** by the management body in its supervisory function was also identified. The management body, both in its management, but especially in its supervisory function, might not have understood the complexity of their business and the risks involved, and consequently failed to identify and constrain excessive risk-taking. Time constraints contributed to the members of the management body in its supervisory function failing to fulfil their duties.

21. The **risk management and internal control frameworks** were often not sufficiently integrated within institutions or groups. A uniform methodology and terminology was missing, so that a holistic view of all risks did not exist. Control functions often lacked appropriate resources, status and/or expertise.

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

2. Purpose and scope of the Guidelines on Internal Governance

23. The EBA's predecessor, the CEBS, had already addressed some of the most significant issues arising from the financial crisis within its **High Level Principles on Remuneration** published in April 2009 and in its **High Level Principles on Risk Management**[7] published in February 2010. However, taking into account the findings of its 2009 survey and recent work by other European and international bodies on corporate governance (especially the Basel Committee's Principles for enhancing corporate governance), the EBA saw merit in enhancing these High Level Principles. Accordingly, guidelines concerning the functioning and composition of the management body as well as the qualifications, appointment and succession of its members, as well as improved principles dealing with the Risk Control function, were added.

[7] Both publications are available on the EBA website.

24. The European Banking Authority has consolidated the majority of its guidelines regarding general internal governance issues in the present Guidelines on Internal Governance, while references were made, where appropriate, to other Guidelines covering more specific aspects of internal governance. The CEBS Internal Governance Guidelines have been reviewed and merged with the High Level Principles on Remuneration and on Risk Management. The Guidelines unify the concepts used, integrate the above mentioned High Level Principles into the context of internal governance and take into account the weaknesses identified in the above-mentioned survey and developments since the publication of the Guidelines on the Supervisory Review Process in 2006 (e.g. group context, systems and continuity).

25. The focus of these Guidelines is limited to internal governance and so excludes other aspects of corporate governance (see 'Section 3. Concepts used in the Guidelines' below). Therefore, it does not cover the roles of external auditors, shareholders or other external stakeholders.

26. Various other CEBS Guidelines (e.g. Guidelines on Validation, Stress Testing and Concentration Risk) cover detailed internal governance aspects for their specific areas. They have not been merged with the present Guidelines, which are limited to principles directly aimed at the sound implementation of internal governance in institutions[8]. All guidelines published by the CEBS can be accessed via the EBA website.

27. By enhancing the implementation of their internal governance framework, it is expected that institutions will become more resilient against adverse market conditions and thus contributing to the stability of the financial sector.

3. Concepts used in the Guidelines

28. **Corporate governance** is a broad concept that can be described as the set of relationships between an institution, its management, its shareholders and other stakeholders. Internal governance is a limited but crucial component of corporate governance, focusing on the internal structure and organisation of an institution.

29. **Internal governance** for institutions[9] in the European Community is covered by **Article 22 of Directive 2006/48/EC,** which requires 'that every

[8] These guidelines are neither concerned with internal provisions that apply to investment services which are included in Directive 2004/39, known as the Markets in Financial Instruments Directive (MiFID).

[9] Institutions referred to in these guidelines are credit institutions and investment firms as per Article 22 of the Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of

credit institution has robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, adequate internal control mechanisms, including sound administrative and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management'. Article 73(3) of Directive 2006/48/EC requires that Article 22 also applies to parent undertakings and subsidiaries on a consolidated or sub-consolidated basis.

30. Internal governance includes all standards and principles concerned with setting an institution's objectives, strategies, and risk tolerance/appetite; how its business is organised; how responsibilities and authority are allocated; how reporting lines are set up and what information they convey; and how internal control is organised. Internal governance also encompasses sound IT systems, outsourcing arrangements and business continuity management.

31. The EBA is aware that within the Member States usually one of two **governance structures** is used - a unitary or a dual board structure. Under a unitary board structure, one body (e.g. the Board of Directors) performs both supervisory and management functions while, under a dual board structure, these functions are performed by a supervisory board and a board of managers respectively. These functions are further described under Title II, chapter B.

32. The Guidelines do not advocate any particular structure. The term '**Management body**' is used in the Guidelines to embrace all possible governance structures. The concept is purely functional, for the purpose of setting out guidance and principles aimed at a particular outcome irrespective of the specific legal structure applicable to an institution in its Member State. Consequently the Guidelines generally do not state whether a particular task or responsibility falls within the management body's management or supervisory function; that will vary according to the national legislation within each Member State. The key point is to ensure that the particular task or responsibility is carried out.

33. The Guideline is consistent with the three-lines-of-defence model. The first 'line of defence' provides that an institution should have in place effective processes to identify, measure or assess, monitor, mitigate and report on risks. These processes are referred to as **Risk Management**.

---

credit institutions (recast) applies; for investment firms see also Article 34 of Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast), hereafter both directives are referred to as the Capital Requirements Directive (CRD)..

34. An institution should as a second 'line of defence' have an appropriate **Internal Control** framework to develop and maintain systems that ensure: effective and efficient operations; adequate control of risks; prudent conduct of business; reliability of financial and non-financial information reported or disclosed (both internally and externally); and compliance with laws, regulations, supervisory requirements and the institution's internal policies and procedures. The Internal Control framework should cover the whole organisation, including the activities of all business, support and control units. The third 'line of defence' consists of the internal audit function, which provides an independent review of the first two 'lines of defence'.

35. In assessing the efficiency of Internal Control within an institution, the management body should be able to rely on the work of **control functions**, including the **Risk Control function**, the **Compliance function** and the **Internal Audit function.** These control functions should be organisationally independent from the units they control.

36. **'Risk tolerance/appetite'** is a term that embraces all relevant definitions used by different institutions and supervisory authorities. These two terms are used here interchangeably to describe both the absolute risks an institution is *a priori* open to take (which some call risk appetite) and the actual limits within its risk appetite that an institutions pursues (which some call risk tolerance).

37. Finally, it should be noted that, besides the background provided here, in between the text of the Guidelines that follows, further explanations on specific aspects of the guidelines are occasionally provided, which either offer examples or explain the rationale behind a provision. Where this is the case, this explanatory text appears in a framed text box.

III. EBA Guidelines on Internal Governance

Status of 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.

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 document are directed primarily at institutions.

Reporting Requirements

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.

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.

In between the text of the Guidelines that follows, further explanations on specific aspects of the guidelines are occasionally provided, which either offer examples or provide the rationale behind a provision. Where this is the case, this explanatory text appears in a framed text box.

Contents

I. Executive Summary 3

II. Background and rationale 7

1. Importance of internal governance 7

2. Purpose and scope of the Guidelines on Internal Governance 8

3. Concepts used in the Guidelines 9

III. EBA Guidelines on Internal Governance 12

Title I -Subject matter, Scope and definitions 16

1. Subject matter 16

2. Scope and level of application 16

3. Definitions 16

Title II – Requirements regarding institutions' internal governance 16

A. Corporate Structure and Organisation 16

4. Organisational framework 16

5. Checks and balances in a group structure 17

6. Know-your-structure 18

7. Non-standard or non-transparent activities 19

B. Management body 21

B.1 Duties and responsibilities of the management body 21

8. Responsibilities of the management body 21

9. Assessment of the internal governance framework 22

10. Management and supervisory functions of the management body 22

B.2 Composition and functioning of the management body 23

11. Composition, appointment and succession of the management body 23

12. Commitment, independence and managing conflicts of interest in the management body 24

13. Qualifications of the management body 25

14. Organisational functioning of the management body 26
Assessment of the functioning of the management body 26
Role of the chair of the management body 27
Specialised committees of the management body 27
Audit committee 28
Risk committee 29
B.3 Framework for business conduct 29
15. Corporate values and code of conduct 29
16. Conflicts of interest at institution level 29
17. Internal alert procedures 30
B.4 Outsourcing and renumeration policies 31
18. Outsourcing 31
19. Governance of remuneration policy 32
C. Risk management 32
20. Risk culture 32
21. Alignment of remuneration with risk profile 33
22. Risk management framework 34
23. New products 36
D. Internal control 37
24. Internal control framework 37
25. Risk Control function (RCF) 38
26. The Risk Control Function's role 39
RCF's role in strategy and decisions 39
RCF's role in transactions with related parties 40
RCF's role in complexity of the legal structure 40
RCF's role in material changes 40
RCF's role in measurement and assessment 40
RCF's role in monitoring 41
RCF's role in unapproved exposures 41
27. Chief Risk Officer 42

28. Compliance function 43

29. Internal Audit function 43

E. Information systems and business continuity 44

30. Information system and communication 44

31. Business continuity management 45

F. Transparency 46

32. Empowerment..... 46

33. Internal governance transparency 46

Title III – Final Provisions and Implementation 48

34. Repeal 48

35. Date of application 48

Title I -Subject matter, Scope and definitions

1. Subject matter

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.

2. Scope and level of application

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.

Explanatory note CEBS/EBA has produced Guidelines on the Supervisory Review Process, which can be found on the EBA website.

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.
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.

3. Definitions

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 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.

Title II – Requirements regarding institutions' internal governance

A. Corporate Structure and Organisation

4. Organisational framework

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.
3. The management body should assess how the 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.
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.

Explanatory note
Changes can result, for example, from the setting up of new subsidiaries, mergers and acquisitions, selling or dissolving parts of the group, or from external developments.

5. Checks and balances in a group structure

1. In a group structure, the management body of an institution's parent company shall have the 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.
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 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.

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.
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.
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 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.

6. A regulated subsidiary should consider having as an element of strong governance also a sufficient number of independent members on the management body. Independent members of the management body are non-executive directors who are independent of the subsidiary and of its group, and of the controlling shareholder.

6. Know-your-structure

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.

Explanatory note
It is crucial that the management body fully knows and understands the operational structure of an institution. Where an institution creates many legal entities within its group, their number and, particularly,

interconnections and transactions between them, may pose challenges for the design of its internal governance and for the management and oversight of the risks of the group as a whole, which represents a risk in itself.

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. It is also responsible for the approval of sound strategies and policies for the establishment of new structures. Likewise the management body should recognise the risks that the complexity of the legal entity's structure itself poses and should ensure the institution is able to produce information in a timely manner, regarding the type, charter, ownership structure and businesses of each legal entity.
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 control functions and supervisors, as appropriate.
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.

7. Non-standard or non-transparent activities

1. Where an institution operates through special-purpose or related structures or in jurisdictions that impede transparency or do not meet international banking standards, the management body shall understand their purpose and structure and the particular risks associated with them. The management body shall only accept these activities when it has satisfied itself the risks will be appropriately managed.

Explanatory note

In addition to that principle, competent authorities may also apply the '*Core Principles for Effective Banking Supervision'*, developed by the Basel Committee on Banking Supervision, when they evaluate business activities in jurisdictions that are not fully transparent or do not meet international banking standards.

The institution may have legitimate reasons for operating in certain jurisdictions (or with entities or counterparties operating in those jurisdictions) or establishing particular structures (e.g. special purpose vehicles or corporate trusts). However, operating in jurisdictions that are not fully transparent or do not meet international banking standards (e.g. in the areas of prudential supervision, tax, anti-money laundering or anti-terrorism financing) or through complex or non-transparent structures may pose specific legal, reputational and financial risks. They may also impede the ability of the management body to conduct appropriate business oversight and hinder effective banking supervision. They should therefore only be approved and maintained when their purpose has been defined and understood, when effective oversight has been ensured and when all material associated risks these structures could generate can be appropriately managed.

As a consequence, the management body should pay special attention to all these situations as they pose significant challenges to the understanding of the group's structure.

2. The management body should set, maintain and review, on an on-going basis, appropriate strategies, policies and procedures governing the approval and maintenance of such structures and activities in order to ensure they remain consistent with their intended aim.
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 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.

4. The same measures should be taken when an institution performs non-standard or non-transparent activities for clients.

Explanatory note

Non-standard or non-transparent activities for clients (e.g. helping clients to form vehicles in offshore jurisdictions; developing complex structures and finance transactions for them or providing trustee services) pose similar internal governance challenges and can create significant operational and reputational risks. Therefore the same risk management measures need to be taken as for the institutions own business activities.

5. All these structures and activities should be subject to periodic internal and external audit reviews.

B. Management body

B.1 Duties and responsibilities of the management body

8. Responsibilities of the management body

1. The management body shall have the overall responsibility for the institution and shall set the institution's strategy. The responsibilities of the management body shall be clearly defined in a written document and approved.

Explanatory note

The sound execution of the responsibilities of the management body is the basis for the sound and prudent management of the institution. The documented responsibilities have also to be in line with national company laws.

2. The key responsibilities of the management body should include setting and overseeing:

   a. the overall business strategy 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 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.

3. The management body should also regularly review and adjust these policies and strategies. The management body is responsible for appropriate communication with supervisory authorities and other interested parties.

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.

10. Management and supervisory functions of the management body

1. The management and supervisory function of the management body of an institution shall interact effectively.

Explanatory note

Member States usually use one of two **governance structures** - a unitary or a dual board structure. In both structures the management body in its management function and the management body in its supervisory function each play their own role in the management of the institution, directly or through committees.

The management function proposes the direction for the institution; ensures the effective implementation of the strategy and is responsible for the day-to-day running of the institution.

The supervisory function oversees the management function and provides advice to it. Its oversight role consists in providing constructive challenge when developing the strategy of an institution; monitoring of the performance of the management function and the realisation of agreed goals and objectives; and ensuring the integrity of the financial information and effective risk management and internal controls.

To achieve good governance, an institution's management and supervisory functions should interact effectively to deliver the institution's agreed

strategy, and in particular to manage the risks the institution faces. While there may be significant differences between different countries' legislative and regulatory frameworks, they should not preclude effective interaction of these two functions, irrespective of whether the management body comprises of one body or more.

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.

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.
4. Each function should provide the other with sufficient information. The management body in its management function should comprehensively inform regularly, and without delay if necessary, the management body in its supervisory function of the elements relevant for the assessment of a situation, the management of the institution and the maintaining of its financial security.

B.2 Composition and functioning of the management body

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 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.
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.

Explanatory note

Where the management body in its supervisory function is formally separate from the management body in its management function, objectivity and independence of the management body in its supervisory function still need to be assured by appropriate selection of independent members.

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 non-compliance 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 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 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.

14. Organisational functioning of the management body

1. The management body shall define appropriate internal governance practices and procedures for its own organisation and functioning and have in place the means to ensure such practices are followed and periodically reviewed for improvement.

Explanatory note
Sound internal governance practices and procedures for the management body send important signals internally and externally about the governance policies and objectives of the institution. The practices and procedures include the frequency, working procedures and minutes of meetings, the role of the chair and the use of committees.

2. The management body should meet regularly in order to carry out its responsibilities adequately and effectively. The members of the management body should devote enough time to the preparation of the meeting. This preparation includes the setting of an agenda. The minutes of the meeting should set out the items on the agenda and clearly state the decisions taken and actions agreed. These practices and procedures, together with the rights, responsibilities and key activities of the management body, should be documented and periodically reviewed by the management body.

Assessment of the functioning of the management body

3. The management body should assess the individual and collective efficiency and effectiveness of its activities, governance practices and procedures, as

well as the functioning of committees, on a regular basis. External facilitators may be used to carry out the assessment.

Role of the chair of the management body

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.

Explanatory note
The chair of the management body plays a crucial role in the proper functioning of the management body. He or she provides leadership to the management body and is responsible for its effective overall functioning.

5. In a one tier system, the chair of the 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.

Explanatory note
Checks and balances could comprise for example, having a lead senior independent member of the management body in its supervisory function or a similar position.

Specialised committees of the management body

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.

Explanatory note
Delegating to such committees does not in any way release the management body in its supervisory function from collectively discharging its duties and responsibilities but can help support it in specific areas if it facilitates the development and implementation of good governance practices and decisions.

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. Each committee should have a documented mandate (including its scope) from the management body in its supervisory function and established working procedures. Membership and chairmanship of a committee might be rotated occasionally.

Explanatory note
The rotation of membership and chairmanship helps to avoid undue concentration of power and to promote fresh perspectives.

8. The respective committee chairs should report back regularly to the management body. 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 chair or a member of one specialised committee might also be a member of another specialised committee.

Audit committee

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.

Explanatory note
See also Art 41 of Directive 2006/43/EC on statuary audits of annual accounts and consolidated accounts.

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.
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

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.

Risk committee

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.

B.3 Framework for business conduct

15. Corporate values and code of conduct

1. The management body shall develop and promote high ethical and professional standards.

Explanatory note
When the reputation of an institution is called into question, the loss of trust can be difficult to rebuild and can have repercussions throughout the market. Implementing appropriate standards (e.g. a code of conduct) for professional and responsible behaviour throughout an institution should help reduce the risks to which it is exposed. In particular, operational and reputational risk will be reduced if these standards are given high priority and implemented soundly.

2. The management body should have clear policies for how these standards should be met.
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.

16. Conflicts of interest at institution level

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.

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 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).
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.
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.

17. Internal alert procedures

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. 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 whistleblower procedure). The alert procedures should be made available to all staff within an institution. Information provided by the staff via the alert procedure should, if relevant, be made available to the management body.

Explanatory note
In some Member States, in addition to any internal alert procedures within an institution, there may also be the possibility for staff to inform the supervisory authority about concerns of this type.

B.4 Outsourcing and remuneration policies

18. Outsourcing

1. The management body shall approve and regularly review the outsourcing policy of an institution.

Explanatory note
The present Guideline is limited to the outsourcing policy, specific aspects of the issue of outsourcing are treated in the CEBS Guidelines on Outsourcing, available at EBA's website. Institutions are expected to comply with both sets of Guidelines. In case of discrepancies, the outsourcing (CEBS) Guidelines shall prevail, as more specific. In case an issue is not covered by the CEBS Guidelines, the general principle of the present Guidelines shall apply.

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.
4. The policy should state that outsourcing arrangements should not hinder effective on-site or off-site supervision of the institution and should not contravene any supervisory restrictions on services and activities. The

policy should also cover internal outsourcing (e.g. by a separate legal entity within an institution's group) and any specific group circumstances to be taken into account.

19. Governance of remuneration policy

1. Ultimate oversight of the remuneration policy shall rest with an institution's management body.

Explanatory note
The present Guidelines provide the *general* framework applicable to the governance of the remuneration policy. *Specific* aspects of the issue of remuneration are treated in the December 2010 CEBS Guidelines on Remuneration. Institutions are expected to comply with both sets of Guidelines.

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 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.

C. Risk management

20. Risk culture

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.

Explanatory note
Since the business of an institution mainly involves risk taking, it is fundamental that risks are appropriately managed. A sound and consistent risk culture throughout an institution is a key element of effective risk management.

2. An institution should develop its risk culture through policies, examples, communication and training of staff regarding their responsibilities for risk.
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.
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.
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.

21. Alignment of remuneration with risk profile

1. An institution’s remuneration policy and practices shall be consistent with its risk profile and promote sound and effective risk management.

Explanatory note
The present Guidelines provide the *general* framework applicable to the alignment of the remuneration policy with an institution’s risk profile. *Specific* aspects of remuneration policy are covered in the December 2010 CEBS Guidelines on Remuneration. Institutions are expected to comply with both sets of Guidelines.

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 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.

22. Risk management framework

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 the business line and institution-wide levels.

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.
3. When identifying and measuring risks, an institution should develop 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.

Explanatory note
The stress test guidelines can be found on EBA’s website.

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.

Explanatory note
For example, an institution should validate a purchased risk model and calibrate it to its individual circumstances to ensure accurate and comprehensive capture and analysis of risk. External risk assessments (including external credit ratings or externally purchased risk models) can help provide a more comprehensive estimate of risk. Institutions should be aware of the scope of such assessments.

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.

Explanatory note

An institution should consider that the results of forward looking quantitative assessments and stress testing exercises are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). For example, models showing very high returns on economic capital may result from a weakness in the models (e.g. the exclusion of some relevant risks) rather than superior strategy or execution by the institution.

7. Regular and transparent reporting 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.
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.

Explanatory note

Effective communication of risk information is crucial for the whole risk management process, facilitates 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.

23. New products

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.
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.
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 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.

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.

D. Internal control

24. Internal control framework

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.
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.
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.
4. An appropriate internal control framework also requires verification by independent 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.

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.
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.

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 on-going basis, and should receive proper training. 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.
8. Control functions should regularly submit to the management body formal reports on major identified deficiencies. These reports should include a follow-up on earlier findings and, for each new identified major deficiency, the relevant risks involved, an impact assessment and recommendations. The management body should act on the findings of the control functions in a timely and effective manner and require adequate remedial action.

25. Risk Control function (RCF)

1. An institution shall establish a comprehensive and independent Risk Control function.
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.

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.
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.

26. The Risk Control Function's role

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.

RCF's role in strategy and decisions

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.
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.
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.

RCF's role in transactions with related parties

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.

RCF's role in complexity of the legal structure

7. The RCF should aim to identify material risks arising from the complexity of an institution's legal structure.

Explanatory note
Risks may include a lack of management transparency, operational risks caused by inter-connected and complex funding structures, intra-group exposures, trapped collateral and counterparty risk.

RCF's role in material changes

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.
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 on the institution's and group's overall risk.

Explanatory note
Material changes or exceptional transactions might include mergers and acquisitions, creation or sale of subsidiaries or SPVs, new products, changes to systems, risk management framework or procedures and changes to the institution's organisation. See the former three Level-3 Committees of European Financial Supervisors (CEBS, CESR, and CEIOPS) joint guidelines from 2008 on the prudential assessment of acquisitions and increases in holdings in the financial sector, which are published on EBA's website. The RCF should be actively involved at an early stage in identifying relevant risks (including potential consequences from conducting insufficient due diligence that fails to identify post-merger risks) related to changes to the group structure (including merger and acquisitions) and should report its findings directly to the management body.

RCF's role in measurement and assessment

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.

RCF's role in monitoring

11. The RCF should ensure all identified risks can be effectively monitored by the business units. The RCF should regularly monitor the actual risk profile of the institution and scrutinise it against the institution's strategic 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.
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.
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.

RCF's role in unapproved exposures

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 remedies.

Explanatory note
Breaches or violations of strategies, risk tolerance/appetite or limits can be caused by new transactions, changes in market circumstances or by an evolution in the institution's strategy, policies or procedures, when limits or risk tolerance/appetite are not changed accordingly.

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.
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).

Explanatory note

For the scope of these guidelines 'fraud' encompasses internal and external fraud as defined in Dir 2006/48/EC, Annex X, Part 5. This includes losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party (internal fraud) and losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party (external fraud).

27. Chief Risk Officer

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.
3. The CRO should have sufficient expertise, operating experience, independence and seniority to challenge decisions that affect an institution's exposure to risk. 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.
5. When an institution's characteristics – 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.
6. The institution should have documented processes in place to assign the position of the 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.

28. Compliance function

1. An institution shall establish a Compliance function to manage its compliance risk.
2. An institution shall approve and implement a compliance policy which should be communicated to all staff.

Explanatory note

Compliance risk (being defined as the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices or ethical standards) can lead to fines, damages and/or the voiding of contracts and can diminish an institution's reputation.

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). 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).
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.
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 institution's activities.
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.

Explanatory note

Special care should be taken when the institution performs certain services or sets up structures on behalf of customers (e.g. acting as a company or partnership formation agent, providing trustee services, or developing complex structured finance transactions for customers) which can lead to particular internal governance challenges and prudential concerns.

29. Internal Audit function

1. The Internal Audit function ('IAF') shall assess whether the quality of an institution's internal control framework is both effective and efficient.
2. The IAF should have unfettered access to relevant documents and information in all operational and control units.
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.
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. 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.
5. The management body should encourage the internal auditors to adhere to national and international professional standards. Internal audit work should be performed in accordance with an audit plan and detailed audit programs following a 'risk based' approach. The audit plan should be approved by the audit committee and/or the management body.

Explanatory note
An example of professional standards referred to here is that of the standards established by the Institute of Internal Auditors.

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.

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.

Explanatory note

Management decision making could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled. Thus a critical component of an institution's activities is the establishment and maintenance of information and communication systems that cover the full range of its activities. This information is typically provided through both electronic and non-electronic means.

An institution should be particularly aware of the organisational and internal control requirements related to processing information in electronic form and the need to have an adequate audit trail. This also applies if IT systems are outsourced to an IT service provider.

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.

31. Business continuity management

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.

Explanatory note

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

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 priorities and objectives.

Explanatory note

Regarding the Operational Risk Management Function see also Directive 2006/48/EC Annex X, Part 3, Par. 4 which requires such a independent function for AMA institutions; the tasks of this function are described in the Guidelines on Validation par. 615-620 (published in 2006) which are available at the EBA website.

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.

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.

F. Transparency

32. Empowerment

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

33. Internal governance transparency

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.

Explanatory note

The objective of transparency in the area of internal governance is to provide all relevant stakeholders of an institution (including shareholders, employees, customers and the general public) with key information necessary to enable them to judge the effectiveness of the management body in governing the institution.

According to Article 72 of Directive 2006/48/EC and Article 2 of Directive 2006/49/EC, EU parent institutions and institutions controlled by an EU parent financial holding company should disclose comprehensive and meaningful information that describes their internal governance on a consolidated level. It is good practice that every institution discloses in a proportionate way information on their internal governance on a solo basis.

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 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.

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.

Title III – Final Provisions and Implementation

34. Repeal

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).

35. Date of application

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.

IV. Accompanying documents

Cost and benefit analysis regarding the Internal Governance Guidelines

Contents

Background 49
Overview on the amendments made 49
Results of the consultation 50
Costs and benefits of the Internal Governance Guidelines 51
Costs and benefits for Institutions 52
Costs and benefits for competent authorities 53
Impact on the economy 54
Conclusion 54

Background

1. The European Banking Authority (EBA) made a large scale review/update of all internal governance principles contained in various Committee of European Banking Supervisors (CEBS) guidelines. The focus was mainly on revamping the CEBS Internal Governance Guidelines, currently still included in the "CEBS Guidelines on the Application of the Supervisory Review Process under Pillar 2" (GL 03), as originally published in January 2006) and in the High Level Principles on Remuneration (published in April 2009) and on Risk Management (published in February 2010) and on transposing BCBS principles on corporate governance into EBA Guidelines on Internal Governance.

2. The European Commission has published a Green Paper on corporate governance in financial institutions. Regulatory proposals were published in July 2011.

Overview on the amendments made

3. All former CEBS guidelines specifically aiming at internal governance have been consolidated into the present Internal Governance Guidelines. The

internal governance guidelines contained in the Guidelines on the Supervisory Review Process (GL03) have been reviewed and merged with the High Level Principles on Remuneration and on Risk Management. The Guidelines unify the concepts used, integrate the above mentioned High Level Principles into the context of internal governance and take into account weaknesses identified in the financial crisis and developments since the publication of the former CEBS Guidelines (e.g. the updated BCBS guidance on "Enhancing corporate governance for banking organisations").

4. The structure of the Guidelines is similar to the previous Internal Governance Guidelines which were composed of four chapters. To integrate the High Level Principles on Risk Management and to introduce additional guidance on Systems and Business Continuity, chapters on "Risk Management" and "Systems and Business Continuity" have been added. Consequently, the Guidelines now contain six chapters, preceded by an "Executive Summary" and a chapter on "Background and rationale" which also contains definitions of the concepts used in the Guidelines. To cover internal governance more comprehensively, the content of the Guidelines has been complemented with guidelines concerning the functioning and composition of the management body as well as the qualification, appointment and succession of its members; guidelines to improve the principles dealing with the risk control function and principles regarding the group context, systems and business continuity.

Results of the consultation

5. On 13 October 2010 CEBS submitted the draft Guidebook on Internal Governance for public consultation - the consultation period ended on 14 January 2011; 15 responses have been received[10]. A public hearing was held in December 2010.

6. Overall respondents have been supportive to the proposed Guidelines and appreciated that the EBA has developed a comprehensive set of internal governance guidelines which is in line with international standards. Respondents also appreciated that the principle of proportionality is applied. Respondents stated that the key issue during the financial crisis was not a lack of governance rules but a lack of effective implementation of these rules. A fully functioning and trusted banking system, supported by sound governance frameworks in institutions, is a key component of any modern economy. Some respondents suggested that the Guidelines should only be applied at group level. The Respondents suggested that the requirements regarding the management body should be spelled out in more detail.

[10] The public responses to CP44 are published on the EBA website together with the initial consultation paper.

7. The Respondents commented that the transparency requirements (information about internal governance) on group and solo level are difficult to meet, in particular in large groups. It would be sufficient to ask for transparency on group level only. This comment has been accommodated and now follows the approach used in article 72 of Directive 2006/48/EC regarding pillar 3 disclosures.

8. Respondents referred to the work planned by the European Commission regarding corporate governance in the financial sector and asked the EBA to consider this, before new guidelines are put in place. In the meantime, the EU Commission published proposals for corporate governance legislation as a part of the CRD IV proposals in July 2011. A first review of the proposals showed that there are no contradictions between the proposed provisions of the Capital Requirements Directive and the Guidelines. The CRD IV contains some more detailed rules regarding the limitation of directorships and the use of committees. However, the CRD IV will only come into force in 2013. The EBA will have to develop regulatory and implementing technical standards for different corporate governance aspects. The EBA intends to go forward with publishing the Guidelines and requiring its implementation by competent authorities by the end of March 2012.

Costs and benefits of the Internal Governance Guidelines

9. During the recent financial crisis, several institutions needed immense financial support from member states to restore the trust in the banking system.

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

11. In recent years, internal governance issues have received more and more attention from various international bodies[11]. Their main effort has been to correct institutions' weak or superficial internal governance practices

[11]See in particular:
BCBS : 'Principles for enhancing corporate governance' of 4 October 2010 available at: http://www.bis.org/publ/bcbs176.htm;
OECD : 'Corporate governance and the financial crisis -Conclusions and emerging good practices to enhance implementation of the Principles' of February 2010 available at : http://www.oecd.org/dataoecd/53/62/44679170.pdf;
European Commission: 'Green Paper on Corporate governance in financial institutions and remuneration policies' of June 2010, available at: http://ec.europa.eu/internal_market/company/docs/modern/com2010_284_en.pdf .

as identified in the financial crisis. These faulty practices, while not a direct trigger for the financial crisis, were closely associated with it and so were a key contributory factor.

12. The cost and benefit analysis takes into account the already existing legislation, in particular Directives 2006/48/EC and 2006/49/EC, the changes made to existing Guidelines within the Internal Governance Guideline and the results of the public consultation.

Costs and benefits for Institutions

13. Institutions and Member States shall make every effort to comply with the Internal Governance Guidelines. Institutions have also to comply with national company laws and with the national implementation of the Guidelines.

14. The Guidelines mainly consolidate former CEBS guidelines. Where they occur, new guidelines are mainly built on best practices established in the banking sector. Furthermore, internal governance matters are by nature part of the organisation of any company, whether in the banking sector or not. The complexity of governance arrangements depends on the size, complexity and strategy of an institution and is not driven by the Guidelines. Therefore, the overall cost impact of the Guidelines on the banking industry should be relatively low.

15. As sound internal governance practices helped some institutions to manage the financial crisis significantly better than others, institutions will benefit from implementing sound governance procedures through a higher resilience. Institution will also benefit in general from the clarification of supervisory requirements and expectations, which are easier to assess, as they are contained in one Guideline.

16. However, the implementation of the Guidelines and changes of respective practices and documentations, as well as some shift in the assignment from staff to improve the risk management and control function, will have some financial impact as described below.

17. Costs will be triggered by raising the qualification and the available resources of the internal control functions. This may add in particular staff costs, which will depend on the size and complexity of institutions. Those costs will result from setting the right incentives for qualified staff to work in those areas, from assigning more staff to those areas and from higher budget needs for systems and training. Institutions will benefit in particular from an improved internal risk control function, as a better management of risks will lead to lower losses related to credit risk, market risk and in particular operational risk. It cannot be estimated which effect would be

higher on the long run. However, an improved internal control framework also protects the reputation of an institution.

18. The qualification and expected time commitment of the management body was clarified in the guidelines. While one might argue that this would cause additional cost, those costs are only needed to establish a sound internal governance. This was already required by existing regulation. However, a stronger supervisory function within institutions may be more costly in terms of staff costs and budget for training, but institutions will also benefit from an improved oversight function, which will lead to a better alignment of the risk profile with the risk appetite as set by the management body.

19. Institutions and groups will have to document policies in a more consistent way. The documentation requirements will cause moderate costs in institutions. If higher costs would emerge, the reason for this would be non-compliance with already existing documentation requirements. Institutions would benefit from better documentation, available to relevant staff, as policies would be better understood and implemented in the day-to-day business.

20. New content was in particular added regarding systems and business continuity management. However, those guidelines, do not impose new rules, but depict already existing best practices in line with the requirements of Article 22 and Annex V of Directive 2006/48/EC. Therefore they should not trigger additional costs in institutions, which would already have implemented appropriate systems and business continuity management procedures, as required by existing regulation.

Costs and benefits for competent authorities

21. Member states shall make every effort to comply with the Internal Governance Guidelines. Competent authorities need to implement the Guidelines. This includes changes to national policy documents as well as changes within the actual supervision of banks.

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

23. Within their supervisory procedures, banking supervisors are used to review the internal governance of institution. As the scope of this review may slightly change, supervisors will benefit from consolidated Guidelines, as the guidelines are easier to access. In addition a few additional requirements in the assessment of the fitness and propriety of directors have to be considered. However, the Guidelines do not change this process

fundamentally. The European Commission includes regulatory proposals in this area.

Impact on the economy

24. The implementation of the Guidelines will improve internal governance within financial institutions and therefore reduce their vulnerability. Sound internal governance and conduct of business helps to build up trust in the banking system.

25. The implementation costs itself are too low, to have any relevant impact on the economy. As the Guidelines do not change the capital requirements, it is not expected that they have any impact on the lending capacity of the banking system or other services offered.

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

Conclusion

27. While the implementation of the Guidelines will trigger moderate one off costs in institutions and competent authorities, the ongoing costs for an improved governance framework and its supervision should be relatively low. Institutions will also benefit from an improved governance framework by a better alignment of the risk profile with the risk strategy/appetite and a better management of risks, which may lead to a reduction of losses. The implementation of the Guidelines will result in a more resilient banking system. Therefore the benefits considerably outweigh the costs.

Feedback statement on the public consultation of the Guidelines on Internal Governance (CP 44) and on the opinion of the Banking Stakeholder Group

1. The European Banking Authority (EBA) officially came into being on 1 January 2011 and has taken over all existing and ongoing tasks and responsibilities from the Committee of European Banking Supervisors (CEBS).

2. On 13 October 2010 the CEBS submitted the draft Guidelines on Internal Governance for public consultation - the consultation period ended on 14 January 2011; 15 responses were received[12].

3. A public hearing was held on 15 December 2010 at the CEBS's premises in London, to allow interested parties to share their views with the CEBS. A summary of the hearing, including the CEBS's responses, is available on the EBA website[13]. In some cases, when a final response was not given, comments were included in this feedback statement as well.

4. Respondents suggested involving the Banking Stakeholder Group (BSG), before publishing the Guidelines. 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 requires that as well as public consultations the EBA shall, where appropriate, also request opinions or advice from the Banking Stakeholder Group.

5. On 27 May 2011 the draft Guidelines on Internal Governance were presented to the BSG. It was concluded that no formal opinion of the BSG was deemed necessary, given that the work started under the CEBS and the public had already been consulted about the Guidelines.

6. Overall, the respondents were supportive of the proposed Guidelines and appreciated the fact that the EBA has developed a comprehensive set of internal governance guidelines which is in line with international standards. The respondents also welcomed the application of the principle of proportionality. The respondents stated that the key issue during the financial crisis was not a lack of governance rules but rather a lack of

[12] The public responses to CP 44 have been published on the EBA website.

[13] A summary of the results of the public hearing has been published on the EBA website together with the initial consultation paper.

effective implementation of these rules. A fully functioning and trusted banking system, supported by sound governance frameworks in institutions, is a key component in any modern economy.

7. Some respondents suggested that the Guidelines should only be applied at group level. The Guideline lays out in more detail the requirements contained in Article 22 of Directive 2006/48/EC , which is applicable to all credit institutions and (via Article 34 of Directive 2006/49/EC) investment firms. If a principle applies by exception only to group or subsidiary level, this is stated in the text of that particular guideline. Article 73(3) of Directive 2006/48/EC states that the requirements of Article 22 must also be applied at consolidated and sub-consolidated level.

8. The respondents suggested that the requirements regarding management bodies should be spelled out in more detail, differentiating between the differing functions of management bodies and the different governance structures (1-tier and 2-tier systems). The EBA refrained from providing this level of detail in its Guidelines, which are not legally binding and need to be implemented by national competent authorities. A functional concept like "management body" is the most appropriate way of ensuring that all the different forms of national company law can be complied with.

9. The respondents also pointed out that the European Commission is working on enhancements to the corporate governance framework for institutions and recommended that the EBA should take these into account. The EBA is fully aware of those developments. In the future, the EBA might develop binding technical standards in this area in coordination with the European Commission.

10. A feedback table is provided below which gives a detailed description of the comments received and the EBA´s responses to them. Some minor drafting changes suggested by respondents have been accommodated without being mentioned in the feedback table.

Feedback table on CP 44: analysis of the responses and suggested amendments

The first column of the feedback table makes reference to the terminology and paragraph numbering used in the original CP 44. The last column refers to the terminology and numbering of the final guidelines.

CP 44	Summary of comments received	The EBA's response	Amendments to the proposals
Guideline on Internal Governance			
General Comments			
		The Guidebook has been redrafted to comply with the EBA's quality criteria for drafting guidelines and was renamed accordingly The format and numbering of paragraphs has changed and an executive summary has been added. The changes concern only the format and structure of the document, but not its content.	
Consulta-tion procedure	Respondents suggested discussing the Guideline with the Banking Stakeholder Group as well once it has been established as provided for under the EBA Regulation.	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 requires that as well as public consultations, the EBA shall, where appropriate, also request opinions or advice from the Banking Stakeholder Group. The publication of the Guideline was postponed to allow sufficient time for the	No change

		Banking Stakeholder Group to provide its opinion on the Guidebook.	
General comment	A respondent encouraged the EBA to achieve even more convergence of supervisory practices. Where possible and applicable, decisions should not be delegated by the Guideline to national supervisors. The EBA should go for a common solution and establish a convergent supervisory practice.	EBA guidelines are not legally binding. Implementation by the competent authorities is required to make the guidelines applicable to institutions. The procedure is regulated in Article 16 of the EBA Regulation. This includes the possibility of not implementing guidelines or parts of them. However, the EBA might develop binding technical standards for some areas at a later stage. Supervisory colleges aim to harmonise supervisory practices.	No change
General Comment	Respondents referred to the work planned by the European Commission regarding corporate governance in the financial sector, and asked the EBA to consider this before new guidelines are put in place.	The EBA is in regular contact with the European Commission and will update the Guideline if needed to be consistent with European legislation. It is expected that the European Commission (EC) will publish proposals for governance legislation in July 2011. Given the fact that it will take a considerable time before any initiatives from the EC in the field of corporate governance for financial institutions become applicable EU legislation, the EBA intends to proceed with publishing the Guideline and requiring its implementation by the competent authorities by the end of March 2012.	No change
General Comment	Participants questioned the status of the "Guidebook" in relation to the "guidelines"/"binding technical standards" under the new EU supervisory structure that will be in force from 2011 onwards.	The EBA does not anticipate any contradictions between the Guideline and future European initiatives, but, rather, elaboration or specification. The Guideline is a legally non-binding guideline (Article 16 of Regulation (EU) No 1093/2010). The Omnibus I Directive states that the EBA may develop binding technical standards in the area of corporate governance. After endorsement by the	No change

		European Commission those standards would become directly applicable regulation.	
General Comment	Respondents stressed the huge number of 'written policies' requirements institutions must comply with (see paragraphs 43, 60, 81, 86, 90, 101, 113 and 148), which will make it difficult to ensure systematic coordination and updating.	It is important to have policies recorded. Otherwise they are not transparent and cannot be monitored. Moreover, policies are even more difficult to coordinate when they are not recorded. The fact that this requirement is mentioned in several places in the Guideline does not of course prevent institutions' internal governance frameworks from being recorded in one overarching document. In fact, the EBA encourages this practice as it would make compliance with Principle 16 ("Assessment of the internal governance framework") much easier.	No change
1. Importance of Internal Governance			
3 to 7	Some respondents felt that the statements on the weak implementation of governance arrangements were too general. Not all banks suffered from such weaknesses; on the contrary, a vast majority of financial institutions, both in the EU and more widely, did not fail and did not need to have recourse to government support.	Paragraphs 3-7, elaborating on the CEBS survey, need to be read together. Not all banks suffered from the same weaknesses, but some weaknesses have been identified quite often. The paragraph "…The survey also revealed that many institutions needed to improve their implementation of the Guidelines …" has been amended to avoid possible misconceptions.	Para. 36 amended
2. Purpose and scope of the Guideline on Internal Governance			
13 General comment	Participants at the public hearing asked for clarification on whether the Guidebook would apply only at group level or to all institutions.	The Guideline is directed at all institutions, including subsidiaries. If any principles apply by exception only to group or subsidiary level, this is stated in the text of that particular principle. The EBA has clarified the scope of	Para. 29 amended

	Some respondents argue that the guideline should only be applied at group level, not at solo level because internationally active financial groups are often centrally organised. To require multiple levels of application may create inefficient duplication. Application at group level only makes coherence of internal governance (IG) (and consistency amongst relevant supervisors) possible.	application by explaining the link between Article 22 of Directive 2006/48/EC (the legal basis for internal governance requirements) and Article 73(3) of Directive 2006/48/EC, which requires that Article 22 be applied at solo and at group level.	
	Other respondents have similar, but not as far-reaching comments. They argue that at solo level, the Guideline should only be applied by significant/material subsidiaries in a group.	If it is in line with the criteria as set out in paragraph 32, group influence is allowed in the field of internal governance. For non-material subsidiaries in particular, this group influence can be more extensive to avoid unnecessary duplication of work. Furthermore, the combined application at group and solo level does not preclude differences between group entities.	No change
	These two comments come back in further, more detailed comments (either the comments suggest replacing the wording "the institution" by "the parent (institution)" or they propose wording more explicitly allowing group influence), for example with regard to remuneration committee, transparency, etc..	The more detailed comments are dealt with further in the feedback table in line with the above reasoning.	No change
	Another comment from an industry member showed support for the combined application (group + solo), but encourages the CEBS, in order to avoid divergent application in the EU, to go one step further in heading for more convergence of supervisory IG practices within	This concern should be dealt with in supervisory colleges.	No change

	the different legal frameworks of the EU.		
General Comment	Some comments argue that the Guideline places extra responsibility and duties on the parent level (e.g. paragraph 36), but does not recognise the parent/group interest (i.e., duties without commensurate rights).	The Guideline does recognise the parent/group interest by allowing group influence (see paragraph 82) as long as the influence is in line with the criteria set out in paragraph 32.	No change
3. Concepts used in the Guidebook			
General comment	Some respondents argue that proportionality should be better explained (for example for smaller banks, for cooperative banks, etc.). The IG Guideline was perceived as being tailored to internally active, complex, financial groups.	The Guideline strikes a balance between setting clear guidelines and allowing enough flexibility to institutions to organise themselves as they consider appropriate, taking into account their own characteristics. Elaborating more on what proportionality means in practice is not possible given the variety of business models, different sizes, complexities and legal forms of institutions. The guidelines do not aim and do not have the legal power to change national company law, which has to be complied with. Therefore the EBA does not see any need to specify guidelines for specific legal forms at European level.	No change
15/16	Respondents pointed out that there are more possible governance structures than 1-tier and 2-tier models, e.g. the Swedish model would be different, requiring three decision-making bodies (shareholder meeting, board of directors, CEO) and a statutory auditor. Thus respondents felt that the Guideline was too detailed to suit all legal corporate structures, even if the principle of proportionality applies, and stressed that sufficient flexible principles	The EBA guidelines have to be implemented by the national competent authorities, which will ensure that the national specifics of company law will be considered. CP 44 pointed to 1-tier and 2-tier systems as they are the ones usually used. However, other structures may be implemented if they are in line with national company law. The Guideline follows a functional approach. The term "management body" embraces all possible governance structures. The guidelines focus on internal governance. This concept excludes the role of external	Para. 32 amended

	were needed to fit all governance structures.	auditors and shareholders.	
15/16	Respondents pointed out that the purely functional concept of a "management body" may cause some problems when implementing the guidelines, as different governance systems exist. It was suggested that whichever of a management body's functions particular tasks or responsibilities of the Guideline are devoted to should be clearly defined and that a differentiation should be made between 1-tier and 2-tier systems.	As company law may differ from country to country, it is not possible to have a clear assignment to the different functions in place in EBA guidelines. National implementation by the competent authorities may take up this point and align the guidelines to national governance systems.	No change
16	Respondents asked for clarification that no shift in responsibilities set within national legislation is intended.	The Guidelines are not legally binding and must be implemented by the competent national authorities before they are applied to institutions. The implementation chapter specified that national law must be complied with.	Para. 32 amended
16	It was suggested that "The crux is that the task or responsibility is fulfilled and is seen to be fulfilled." be added.	Appropriate documentation is already required from institutions. The supervisory assessment will be based on this and other measures. The suggested addition is therefore not needed.	No change
4. Implementation of the Guidebook			

21	Respondents stated that it was not clear what was meant by "large and complex institutions". To avoid any misunderstanding with regard to the scope it was suggested that this phrase be deleted. This is covered sufficiently in point 22 (principle of proportionality).	The comment was accommodated.	Para. 26 amended
22	Respondents appreciated that the principle of proportionality applied to the Guidebook. To be adequately flexible it was suggested apply the principles on a comply or explain basis.	EBA guidelines are not legally binding. They will be implemented by national authorities; the rules implemented in turn will be applied to institutions. The EBA will conduct an implementation study. During the public hearing the difference between principles (bold text) and explanatory notes in the Guideline was explained. The principles contain the desired outcome, against which the IG framework of an institution will be measured. The explanatory text elaborates on how an institution can reach the outcome, but alternative approaches taking national requirements into account are also possible. It is an institution's own responsibility to propose to its supervisor(s) an IG framework that is tailored to its own characteristics, provided that the objectives are achieved.	Title I, 2.4 amended
24	Respondents requested sufficient time to implement the guidelines and suggested extending the implementation period.	The implementation date is a mandatory date for the implementation of the guidelines within national regulatory frameworks by the competent EU authorities and is not directly applicable to institutions. Once implemented, the guidelines will be applied by the competent authorities - this usually includes a sufficient timeframe for implementation. However, as the Guideline mainly consolidates existing guidelines and only contains	No change

		a limited number of new requirements, the EBA does not see any need to define transitional arrangements.	
A. Corporate structure and organisation			
33	Regarding the "element of strong governance ... to have independent members on the management body" of a subsidiary: Respondents commented that the requirement was not compatible with some national company law and required sufficient flexibility.	National legislation needs to be complied with. However, also having independent directors at subsidiary level is a strong element of internal governance which may be desirable where possible. The Guidebook's wording regarding this issue only states best practice. This was clarified in paragraph 33.	Title II, 5.6 amended
	Other respondents argued that independent directors did not always offer the best possible guarantee for sound governance at subsidiary level, because they were often not familiar with the business or with the operating procedures.	If fit and proper requirements are correctly complied with, independent directors can offer much added value to discussions in management bodies, even though they may not be familiar with daily operations.	No change
	This principle is difficult to apply to most subsidiaries wholly owned by parent institutions.	This is a situation in which independent directors can be most useful in monitoring potential conflicts of interest between subsidiaries and parent institution.	No change
	Other comments supported the best practice but would limit it to certain subsidiaries.	The EBA narrowed the scope of paragraph 33 to regulated subsidiaries.	Title II, 5.6 amended
37-39	Respondents asked that "The management body" be specified to make clear that the	See the responses on the concept of "management body" under chapter 4 and the responses to comments on	No

	requirements in these paragraphs did not fall under the responsibility of the supervisory function.	Principle 6 on the management and supervisory function.	change
41	Specific wording was proposed for paragraph 41, second bullet point: information should be "available" to boards and supervisors "in accordance with applicable law".	Applicable law has to be complied with in any case; the availability of the information will usually be met through a reporting line.	No change
42	Respondents commented that relations between an institution and its customers were not a question of internal governance. Moreover, the tasks required in connection with the performance of certain activities for institutions' clients are not sufficiently clear.	The purpose of this requirement – avoiding operational and reputational risks to an institution – has been clarified.	Title II, 7.4 amended
	One respondent proposed replacing the word "same" in paragraph 42 by "similar" measures.	The word "same" has been retained because "similar" would water down the requirement. The paragraph refers to the activities performed by an institution.	No change
Principle 1 and 3	Respondents argued that internationally active financial groups are necessarily complex. Complexity therefore is a feature of an institution's organisation that must be managed and understood, rather than one to be doctrinally avoided or actively reduced.	Supervisors have an obvious interest in having clear and transparent structures for institutions. Group structures should not hinder effective prudent supervision. The Guideline is not as such against complex structures. As long as institutions can understand and justify their structures, restructuring is not required. Furthermore, restructuring is only a measure of last resort; other, less intrusive measures can be applied by supervisors (e.g. requiring additional checks and balances in a structure).	No change
B. Management body (Principle 5-10)			

Principles 5+6	Respondents asked for further clarification regarding the nature of the duties performed by boards in the unitary board paradigm, and suggested drawing a clear line between the duties of boards and the duties of senior management. Respondents commented that the management function being referred to in Principle 6 was actually the function performed by senior management when making proposals to a board for an institution's direction and then ensuring the effective implementation of the strategy through the day-to-day running of the organisation. The board as a whole is not responsible for the day-to-day running of a institution.	The EBA Guideline follows a functional approach and has no intention of specifying senior management responsibilities regarding the day-to-day business of institutions. Its scope is limited to the responsibilities of the management and supervisory functions of the management bodies. The management body of an institution has the ultimate responsibility for its wellbeing and activities.	No change
Principle 5	Respondents stated that the principles are still too much based on a monistic system. The exclusive reference to 'management body' was perceived as confusing. The term 'management body' refers to boards in both their supervisory and executive functions. This is not efficient and practical. It is essential to make a clearer distinction between decision-making and supervisory functions. Respondents suggested referring to a dualistic system, i.e. separating supervisory and management functions, and specifying the principles accordingly and using another term for 'management body' which is more neutral,	The term "management body" is indeed used to cover all possible governance structures. The guidelines focus on the desired outcome and not on which governance structure in required in the company law of a Member State. Therefore it is not possible to have a clear assignment to the different functions in place in European guidelines. National implementation by the competent authorities may take up this point and align the guidelines to national governance systems. The EBA considered amending the guidelines using the "Solvency 2 language" of "administrative, management or supervisory body" to cover a single board in a one-tier system and the management or supervisory boards in a two-tier system, but came to the conclusion that the	No change

	such as 'board of directors'. This term was used in the Commission Green Paper on Corporate Governance.	functional approach used in the guidelines made this unnecessary. While the Green Paper did use "boards of directors", this is not the language used in European Directives such as the Capital Requirements Directive (CRD) (see e.g. Directive 2006/48/EC, Annex V, point 1).	
Principle 5	Respondents suggested that these responsibilities should apply in their entirety at group level, with more proportionate application at the (regulated) subsidiary level. Internal governance procedures established at group level will, in all but the rarest cases, be sufficient to discharge the responsibilities of the subsidiary management body.	See comments under point 2 of the overview. Consequently Principle 5 stays unchanged.	No change
	Respondents stated that this in particular should not be the responsibility of the regulator; although the regulator should fittingly be interested in how these parameters are set.	Regarding the last comment, responsibilities lie with the management bodies. This is explicitly stated in Principle 5.	No change
43-45	Respondents stated that in cooperative banks certain decisions were made under the auspices of a general assembly. In the statutes of cooperative banks the powers and responsibilities of the members of each of the governing organs are included. The responsibilities of the supervisory and management boards are therefore already described in detail in the various national rules. Therefore respondents did not consider it	Paragraph 43 says there should be a written document setting out the responsibilities of the management body. It does not say where that document has to originate from. So if certain responsibilities are set out/approved elsewhere that document will suffice (or the relevant material can be attached to or kept with any material on other responsibilities decided on by the management body). However, national legislation alone is not sufficient. A written document is intended to ensure and document the fact that a management body is aware of	No change

	necessary to have any additional documentation.	its responsibilities.	
45	Respondents suggested indicating that senior management would have the primary responsibility for appropriate communication with supervisory authorities.	It is clear (e.g. contained in directives) that responsibility rests with management bodies. In practice, it is less likely that the actual tasks might be performed by the members of a management body themselves.	No change
Principle 6	A respondent pointed out that the term "supervisory function" could create confusion. The words "challenge" and "oversight" are used in the supporting text. It was suggested that the term "supervisory function" be replaced by the "challenge and oversight function".	The concepts of management body, management and supervisory function are consistently used in the guidelines. The concepts used are explained in the introductory chapters.	No change
Principle 7 – General	A respondent explained that according to national laws, shareholders alone have the authority to propose appointments to boards of directors. In terms of qualifications, members of governing bodies must have experience adequate to the size and operational complexity of the relevant company. It was pointed out that submitting policies to shareholders would raise awareness regarding the qualifications needed in addition to the professional requirements prescribed in domestic laws.	The scope of the internal governance guidebooks does not include the relations of institutions to their shareholders. However, the absence of a respective guideline should not hinder an institution from making policies available to shareholders or stakeholders.	No change
Principle 7	Respondents asked for clarification on whether this would only apply to management bodies in their management functions and felt that this should apply to executive management. For	The term "management body" refers to both functions. However, in practice there is certainly a greater focus on the management function, but this should not mean that this issue is not relevant to the supervisory function as	No change

	supervisory functions such a procedure would be inappropriate.	well.	
Principle 7	Respondents believe that it is best practice for an organisation to periodically assess its management for each position in order to provide continuity in the conduct of business (the so called 'management replacement matrix').	The principle applies to the management body. It was specified that the paragraph referred to "nominations" for re-appointments. However, the EBA would have no objections if an institution made such performance assessments more often.	Title II, 11.4 amended
52-53	Respondents appreciated that the CEBS acknowledges in paragraph 52 that it should be sufficient for a board to collectively dispose of adequate knowledge and experience. Instead of defining a rigid profile for individual candidate board members in recruitment policies, which would not ensure the requisite diversity within a board, respondents agreed to adopt a principle which should ensure that boards of directors have the collective knowledge, skills and understanding of the business to enable them to contribute effectively.	While the guidelines do not define individual profiles, it is also important that individual members be qualified and experienced (see also paragraph 53). However this does not imply a specific individual profile.	No change
54-55	Respondents requested that paragraphs 54 and 55 be clarified. • A board should include a mix of skills/competencies to allow the board to function competently as a whole, i.e. not all attributes should be required of each individual board member. Board diversity as advocated by the UK Corporate Governance	Regarding the first bullet point, we refer to paragraphs 52-53 of the Guidebook, which are in line with the expressed views. Regarding the second bullet point, the Guideline only refers to an appropriate period, which needs to be in line with national company law. The EBA is of the view that long-term service is not a problem per se.	No change

	Code requires that a board include a broad range of skill sets which will allow a broad range of views to be expressed in order to counter group-thinking. • It does not make sense for board members to serve a defined term at subsidiary level (where they are most likely to be serving "at will"). We do not consider long service of the members of the management body to be a problem per se.		
54-55	Respondents commented that paragraph 55 seemed to imply that board members should be prevented from serving for more than one 'contractual' period and asked for clarification. As long as a board member's performance remained strong and company law requirements in relation to re-election to the board have been fulfilled, respondents saw no need for the enforced retirement of individual board members.	The guidelines do not aim to restrict the re-election of members. However, institutions need to consider the expiry date of contracts, as re-election is not automatic.	No change
56-57	Respondents believe that it is the responsibility of the executive team to develop and implement an institution's strategy, having had the necessary robust discussion at board level with non-executive directors. Executive and non-executive directors should be able to exercise independent judgment about a business as a whole. Respondents pointed out that the limitations of what can be achieved by non-executive directors must be recognised; no	The responsibilities with respect to the setting of strategies are contained in Principle 5 of the Guideline. The management function should develop the strategy which it implements, after it has been agreed by the supervisory function. The supervisory function might consider in its oversight role whether the management function is meeting its responsibilities competently and, if not, take the necessary action. Thus it is also important to have a strong supervisory function. The Guideline does not impose a limit for or a maximum number of different	No change

	amount of robust internal governance processes can make up for a weak executive team. Some non-executive directors may serve in an advisory capacity on public bodies. Respondents do not believe that this service to the community should be discouraged by including it in the count of the number of secondary professional activities a board member holds. The issue is not the number of other positions held per se, but the ability of the director to meet the time commitment. As this is covered adequately in paragraph 56, respondents suggested deleting the first sentence of paragraph 57.	activities, so that this should not discourage service to the community. However, it is of key importance that members of the supervisory function dedicate sufficient time to enable them to fulfil their role within an institution.	
57	Respondents commented that paragraph 57 reads as if all board members are non-executive directors, which cannot be the case and that with non-listed subsidiary directors it is usual for all, or a high percentage, to be executives because of their role within the firm. It would also be common for such executives to serve on multiple group boards.	'Management body' is used in a functional concept. In a 1-tier system, it is obvious that some directors need to fulfil a management function. However, such members also need to be able to devote sufficient time to their duties. Institutions (including non-listed subsidiaries) need to have an appropriate supervisory function irrespective of the governance structure.	No change
58	Respondents pointed out that verifying and evaluating the number of similar positions held by board members is a general principle contained in the codes of best practice on corporate governance which are applied by the large majority of listed European companies. Considering the differences in the dimension and complexity of both the financial companies	The Guideline reflects the best practices mentioned by requiring institutions to challenge how an individual member will spend sufficient time. Paragraph 58 does not specify a limit on the numbers of positions or minimum amount of time, which may differ according to the principle of proportionality and can be set by institutions, which should indicate a minimum expected time commitment. Institutions should be able to explain	No change

	which will implement the rule and those other companies in which directors may cover a similar position, respondents preferred not to refer to a minimum expected time commitment for the members of management bodies (see paragraph 58), but to set up a general principle on this matter.	deviations.	
58	Respondents suggested that auditors should monitor the minimum expected time commitment for all members of the management body.	Devoting sufficient time is the responsibility of the members of management bodies and cannot be delegated to internal or external auditors. More transparency on time devotion would be beneficial.	No change
58	Respondents commented that the requirement for a sufficient time commitment is only applicable to a management body's supervisory function, since the management function is normally a full-time occupation. Respondents questioned whether this provision was reasonable, as responsible candidates should be able to estimate the amount of time demanded.	The provision was kept, as experience has shown that there can be a lack of dedicated time in the management function as well.	No change
59	Respondents pointed out that there were different definitions of independence and that the requirements of this paragraph might be in conflict with national legislation.	The EBA is aware that there are different levels of independence. The supervisory function needs to be sufficiently independent to achieve its objectives. Given that company law differs in each country, a definition of required independence cannot be given. National legislation needs to be obeyed. However, having a sufficient number of independent members in the supervisory function is considered to be best practice.	No change

60	Respondents raised concerns regarding the first bullet point in paragraph 60. Disclosed conflicts of interest that can be managed (e.g. an at-arm's-length transaction) may be acceptable. Requiring that all conflicts of interest should be "avoided" to the extent possible is tantamount to saying that such transactions should not be made. It was suggested that the language state that it is a member's duty to avoid conflicts of interest that have not been disclosed to and approved by the board, but in all other cases to ensure that conflicts are managed appropriately.	The comment was accommodated.	Title II, 12.6.a amended
Principle 9	Respondents stated that there would be no formal qualifications that are uniformly recognised throughout the EU that would demonstrate the necessary levels of knowledge to be able to undertake the role of a non-executive director. It should be up to a board – led by its chairman – to make an assessment of the competencies that a potential new member of the management body could bring, and that there is real benefit in having a diversity of knowledge, experience and understanding available to it. Therefore it was suggest that Principle 9 be amended as follows: "Members of the management body should have sufficient knowledge and understanding, be and r	The process stated is in line with supervisory expectations under a 1-tier system. However the suggested re-wording might give rise to the interpretation that continuity of sufficient knowledge is not needed. The latter is also important (e.g. regarding new products). The paragraph stays unchanged, as it is also in line with other international governance standards (i.e. the Basel document on Enhancing Corporate Governance). More details on the principle are provided in the subsequent paragraphs of the Guidebook.	No change

	emain qualified, including through training, for their positions. They should have a clear understanding of their institution's governance arrangements and their role in them."		
Principle 9	Other respondents suggested setting out the qualifying criteria for board members in more detail and applying them at group and subsidiary level.	A higher level of detail cannot be provided in the Guidebook. It is for management bodies to determine criteria in the light of an institution's business needs and the risks faced.	No change
Principle 9	A respondent suggested implementing a single certificate for the members of management bodies in order to create a level playing field regarding fit and proper requirements. It was also suggested that guidelines be issued which would lead to training programmes for a "European Certified Director".	The required qualifications of members of management bodies and their training needs differ, as the required knowledge and experience profiles differ depending on the size and complexity of the institutions concerned and their business activities. The principle of proportionality applies. The definition of a required knowledge profile and setting up appropriate training programmes is the responsibility of the institutes. Besides "knowledge", other criteria also apply.	No change
64	Respondents suggested amending the phrase "sufficient qualifications" in Paragraph 64. This should be amended to read "skills, knowledge and understanding". In addition, Paragraph 64 should be a collective test, as an individual test would inhibit the appointment of people with diverse backgrounds.	The first suggestion was partly accommodated in paragraph 61, where the elements that could fall under the term "qualifications" are grouped together. However, the requirement does not contain a test as such; there should rather be a sound process to achieve this outcome. The guidelines allow for diversity in the individual profiles of members.	Title II, 13.5 amended
64	Respondents commented that processes to ensure that a given management is sufficiently qualified should be developed comprehensively. The Guideline neither indicates whether	The onus for ensuring that an institution has sufficient qualified management body members and defining appropriate processes to ensure this falls on the institution itself. The process needs to ensure that all the	Title II, 13.5 amended

	institutions or supervisors are the addressees of this rule nor how this process works in the view of the EBA.	requirements on qualification mentioned in Principle 9 are fulfilled on an ongoing basis. The competent authorities will also take into account the guidelines when they assess the fitness and propriety of the members of a management body and the related procedures.	
65	Respondents stated that it seems only natural for the members of a management body to keep up and develop the knowledge that pertains to their level of responsibility. This would not necessarily have to result in costs and time-consuming "individually tailored training programmes" that could also be misused.	It is important for members of a management body to receive an appropriate initiation and to have access to training programmes. The need to develop knowledge and therefore the necessary time and resources may differ between members. Individual training is assumed to be more acceptable and less time consuming for the members of a management body. However, the guidelines do not restrict institutions from having additional training measures in place.	No change
65	Respondents suggested deleting the examples given in paragraph 65, as there was a danger that the areas to be covered in paragraph 65 would end up being a prescriptive list.	A binding list of obligatory training areas was not intended. However, the EBA does not think a change is needed, as the wording "might be covered…" is sufficiently open.	No change
Principle 9 68	Respondents did not disagree with the recommendation of having recourse to an external advisor to evaluate the individual and collective efficiency and effectiveness of an institution's activities, governance practices and procedures, as well as the functioning of committees. However, considering the very different dimensions, complexities and national legal frameworks of the banks which would have to implement such a proposal, respondents stated that it seemed appropriate	The Guideline will be implemented by the competent authorities within the European Union. The review of governance procedures is necessary to ensure compliance with regulatory requirements (e.g., as set out in Article 22 of Directive 2006/48/EC).	No change

	not to set up specific rules on the contents and procedures for evaluating a board (namely not providing for a mandatory procedure). Rather, general principles should be defined which are aimed at facilitating Europe-wide implementation.		
71	Respondents suggested that the guidance in Paragraph 71 be amended to indicate that the Chairman and the CEO should not be the same person "unless the board determines that it would be in the best interests of the enterprise".	This is implicit in the existing wording.	No change
71	Paragraph 71 recommends that the chair of a management body and the CEO should not be the same person. Respondents stated that there is neither empirical evidence nor academic agreement about which of these two formulas is better than the other, as each of them has advantages and disadvantages for institutions (clear leadership or not, lack of proper checks and balances, etc.). Although it is a mere recommendation and not a compulsory, respondents suggested eliminating or, at least, rewriting in such a way that the CEBS would not consider one as more appropriate than the other, regardless of the recommendation of having certain measures in place for cases where the same person had both responsibilities was maintained.	The EBA believes that it is good practice for the roles to be split (unless a good case to the contrary can be made). See also comment above.	No change

72	Paragraph 72 states that "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". Respondents believe that in the case of large, highly complex banks, it should be considered whether creating specialised committees within a board of directors would benefit a board's activities through proposing and consultative functions. Apart from larger and very complex banks, the organisation and set-up of committees should be accomplished in accordance with the complexity and size of the banks concerned.	The principle of proportionality also applies with respect to the requirement to set up specialised committees.	No change
72	Respondents saw particular merit in audit committees and in risk committees and in the cooperation and information flows between the two committees. Respondents suggested that interaction could be assured through the cross-participation of members and by the same Chairperson chairing both.	Having the same person as chair of the audit and the risk committee would call into question the independence of the audit committee chair.	No change
72	Respondents recommended that paragraph 72 should also refer to the need to take into account "any group controls applicable to the relevant subsidiary (if it is not a parent entity)".	As the principle of proportionality applies, a direct reference is not necessary. When considering whether committees should be set up, management bodies will, alongside other aspects, also consider existing controls, including group controls and related information flows.	No change
Principle 10	Respondents pointed out that a board as a whole (collegial body) should continue to be in	As already stated in the text, the responsibilities of management bodies remain unchanged by the presence	No change

72, 75, 78	charge of the oversight of risk management, but indeed with the possibility (no obligation) of setting up a separate risk committee or a similar committee within the board. A board's joint liability towards its shareholders must be maintained. The role of committees within boards is and must remain purely advisory, reporting exclusively to the boards.	of risk committees.	
72	Respondents considered the setting up of committees not to be a responsibility of the supervisory function.	The EBA considers the committees, as explained in the Guidebook, to be a responsibility of the supervisory function. We refer to the explanations of the different governance structures (1-tier, 2-tier systems) provided. This does not of course preclude specialised management teams being set up.	No change
73	One respondent did not agree that there was a need for "a sufficient number of independent members" for committees established at unlisted subsidiaries (assuming that "independent" implies non-executive directors). It was proposed that the scope for this requirement be limited to listed companies.	The CRD applies to all institutions, regardless of whether they are listed companies or not. Having a sufficient number of independent members in committees is a strong element of internal governance. National rules and the principle of proportionality need to be considered. In subsidiaries "independent" may include members from elsewhere in the group to some extent. Institutions should discuss this issue with the competent authority.	No change
73	Respondents supported the explicit formalisation of documentation on the practices and procedures of management bodies and believed that these should be disclosed, but only at the level of parent financial holding companies. Internal governance procedures that apply in regulated subsidiaries of parent	The transparency requirements of the CRD apply only to parent institutions. However, it is good practice for every institution to disclose in proportionate way information on their internal governance on an individual basis. The Guideline has been amended accordingly.	Title II 14.6 and 34.2 amended

	financial holding companies should very closely, if not exactly, mirror those of the parent. Respondents suggested that regulated subsidiaries should not need to disclose their own established committees and their mandates and composition.		
75	Respondents suggested referring to the full scope of activities of the audit committee, as stipulated in Article 41 of Directive 2006/43/EC, as this scope relates directly to the three key areas within the internal governance area: internal control, risk management and internal audit "[…] the audit committee shall, inter alia: monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems […]".	The comment was accommodated.	Title II, 14.9 amended
76	Respondents suggested that the guidance be qualified with the clause "unless the board determines that the most suitable candidate, given the enterprise's circumstances, requires an experienced person even at the cost of some quantum of formal independence." The board should have the flexibility and the final responsibility to make such determinations.	Having an independent chair is best practice. Institutions may discuss differing decisions with their supervisor, if they are in line with national requirements.	No change
78	Respondents commented that in paragraph 78 the Guideline assigns missions to management bodies in their supervisory function, or to risk committees, while it seems that this is not their	The guideline aims to strengthen the oversight role of the supervisory function. Therefore the supervisory function will usually receive information from the risk control function (and the CRO) via the management function.	No change

	role. The committees are merely emanations of a management body in its supervisory function and it is the management body which ultimately holds the decision-making power. Thus, it should be clear that the risk control function (as well as the Chief Risk Officer (CRO) should not have direct access to a board committee (or to the board) without the approval/knowledge of the CEO. The CRO reports to the CEO and cannot be independent from him. The chain of command must be clear and should not be challenged by any direct reporting to the board. When examining the risk exposure of a bank, the board can call the CRO to report to the board in the presence or not of the CEO, but on the basis of information also made available to him/her.	The supervisory function can request any information needed from the risk control function. However, in exceptional cases, the CRO should have the right to inform and access the supervisory function directly, without possibly being interfered with by, e.g., a dominant CEO. This reasoning is covered by the third bullet point of paragraph 120: "The head of the control function generally should report directly to the management body ...". See also the comment for paragraph 120.	
Principle 11 79-81	Respondents stated that management bodies should receive information on the effective implementation and respect of the code of conduct within an organisation on a regular basis.	Paragraph 80 contains a similar requirement; the EBA clarified the wording so that both implementation and compliance with those standards are covered. It is important for management bodies to receive the results of such reviews, which may be performed by another function.	Title II, 15.3 amended
Principle 12	Respondents commented that only unmanageable conflicts of interest need to be prevented; therefore respondents suggested amending the text of the principle as follows: "conflicts policies should identify actual and potential conflicts of interest so that they can be prevented or managed".	See comment for paragraph 60.	Title II, 16.1 amended

79	Respondents suggested adding the following phrase to the first line: '… is called into question, due to employees' misbehaviour, the loss of trust.'	The suggested wording would be too restrictive: e.g. the behaviour of management can also lead to a loss of reputation. The suggested wording was therefore not added.	No change
80	Respondents suggested replacing 'operational risk' with 'reputational risk'.	A code of conduct can reduce operational risks and reputational risks. Although reputational risks are already mentioned in paragraph 79, for clarity's sake the EBA added reputational risk to line 3 of paragraph 80.	Title II, 15.1, Text in box amended
81	Respondents believe that significant suppliers/partners and government officials should be considered in the list of relationships within a code of conduct as defined in paragraph 81 and suggested extending the conflict policy to transactions with related parties (see paragraph 130).	The list within paragraph 81 is not an exhaustive list of possible areas of conflicts of interest. Nevertheless the comment was partly accommodated and the list amended.	Title II, 16.2 amended
Principle 13	Respondents suggested rewording Principle 13 as follows: "appropriate internal procedures allowing staff to confidentially report internal governance concerns."	The term "internal alert procedure" is a generally accepted concept, therefore no change is needed.	No change
84	Respondents stressed that internal alert procedures should respect the confidentiality of the staff that raise such concerns. Concerns need to be raised confidentially e.g. through a whistleblower hotline.	The EBA has added the phrase 'through an internal whistleblower procedure' to paragraph 84.	Title II, 17.2 amended
84	Respondents suggested replacing 'in writing' by 'in durable form', because staff are often made	The EBA has accommodated the comment by deleting the phrase 'in writing'.	Title II, 17.2

	aware of the procedures by use of an intranet.		amended
85	Respondents believe that the possibility for staff to inform the supervisor is an internal company matter. Internal whistleblower processes are sufficient. One respondent suggested deleting this point as it clearly did not represent best practice.	The EBA has described a practice in some Member States without defining it as best practice. The Guideline neither requires such a procedure nor restricts it.	No change
Principle 14	Respondents suggested that outsourcing policies should be the responsibility of senior management (including committees) or their delegates who run the day-to-day operations of an enterprise.	The outsourcing of high-level policies should be adopted at management body level, although day-to-day operations are the responsibility of senior management. Outsourcing can result in significant risks The management body has the ultimate responsibility for ensuring that risks are appropriately managed.	No change
Principle 14	Respondents suggested that outsourcing policy should only concern a bank's core business activities and not all types of outsourcing.	Regarding the scope of possible outsourcing we refer to the CEBS Guidelines on Outsourcing (published December 2006).	No change
Principle 15, 90-94	Respondents suggested taking account of the influence of group-wide policies. Another respondent suggested including only a reference to Financial Stability Board (FSB) Principles and Standards instead of reporting a subset of specific clauses, in order to avoid possible confusion.	The Guideline does not contain any new principles on remuneration, but summarises the CEBS guidelines on remuneration. Paragraph 94 refers explicitly to the CEBS guidelines for more detailed information, including the application of the remuneration principles in a group context.	No change
95	Respondents suggested that managers should at least report annually to supervisors on the assessment and effectiveness of an institution's governance.	The competent authorities will assess the appropriateness of institutions' internal governance in their Supervisory Review and Evaluation Process. The results of such risk assessments will be discussed in supervisory colleges if applicable. During their evaluations, supervisors will	No change

		require appropriate documentation.	
95	Respondents felt that an annual review of internal governance arrangements would be too burdensome, in particular for small institutions, and suggested changing the wording to "periodical". The principle of proportionality should be applied.	Institutions need to have appropriate internal governance arrangements at any time. A yearly review of the arrangements aims at ensuring that sufficient management attention is given to this issue. Smaller institutions often have a less complex governance structure, which is easier to review. Furthermore, reviews can often be limited to considering any changes which have taken place in the intervening period.	No change
C. Risk management			
Principle 17	Respondents believe that the CEBS is using the term 'institution-wide' to apply to parent financial holding companies and their (regulated) subsidiaries and would appreciate confirmation of this. Respondents believe that a risk culture should be homogenous and embedded throughout a whole group.	The Guideline applies to all institutions. The risk culture should be developed at both solo and consolidated levels. The proportionality principle allows financial institutions to adapt the development and the implementation of this risk culture to their own structural specificities. Regarding the group context, we refer also to Chapter A of the Guideline and the respective comments provided.	No change
97	Respondents stated that the third sentence should not be interpreted as giving to the management body in this supervisory function the responsibility for overseeing risk management on a day-to-day basis, as this would be totally unrealistic.	This sentence assigns responsibility for overseeing day-to-day risk management to business units. The EBA feels that the paragraph is clear enough and should not be misinterpreted to mean that this is a day-to-day task of the management body.	No change
100	Respondents suggested that the guidance in Paragraph 100 should make clear that there is no need for external review. The risk management framework will be subject to the	The paragraph was amended; the risk management framework should be subject to independent review.	Title II, 21.6 amended

	oversight of the risk committee (taking account of the factors listed) and can also be reviewed independently by internal audit.		
Principle 18 and Principle 15	Respondents generally agree with the principles regarding the governance of remuneration policy as set out in the FSB Principles and Implementation Standards and the Capital Requirement Directive. However, in order to avoid possible confusion or overlap due to multiple sources and possible differences in wording, interpretation or application, respondents suggested that Principle 15 should only contain a reference to these key regulatory documents without reporting a subset of specific clauses. For example, the wording regarding "staff whose responsibilities have a material impact on the risk profile of an institution" is different from the CRD and CEBS texts and superfluous in a context where further reference for details is in any case made to the full Guidelines.	Principle 18 is in line with the CEBS guidelines on remuneration and remuneration policies (published in December 2010) and stresses the content relevant in this context. Paragraphs 102 and 104 have been aligned with the CRD text in Annex V, new points 23 and 24. Regarding Principle 15, please see comments to Principle 15 in the feedback table above.	Title II, 22.1 text in box amended
109	Respondents stated that exemptions from the risk management framework should be allowed for basic/simple transactions.	It is not clear which basic/simple transactions should be excluded from having a risk management framework. Basic/simple transactions like mortgages or consumer loans have proved to be critical risks for credit institutions. Each institution is responsible for implementing an appropriate risk management framework, taking into account the principle of proportionality, which should provide for sufficient flexibility.	No change

Principle 19	Respondents believe many groups will have substantial subsidiaries and that these will need to consider both their own risks and the benefits they could derive from the work of a firm-wide committee/framework.	The Guideline is applicable to all institutions. Regarding the group context we refer in particular to Chapter A.	No change
Principle 20	Respondents suggested that new products should be approved by CEOs, and also, potentially, CROs, at individual institutions and at group level.	Principle 20 requires that institutions have a well-documented new product approval process in place. The risk control function should be involved in that process, to ensure that risks are assessed properly. New products should be approved for all institutions using them, a single approval at group level is not sufficient. Regarding the role of CROs, we refer to Principle 24.	No change
Principle 20	Respondents agree on the need for a robust new product approval policy, but believe that this will flow from the parent companies, and that it should be the responsibility of their boards to ensure that this is embedded throughout their regulated subsidiaries. Individual subsidiaries should not be required to develop their own policies, but to adopt those set centrally.	In principle we agree, but subsidiaries should not adopt central procedures only as a formality, or central procedures which do not fit their structures, activities or specificities. Subsidiaries may adopt central procedures but their management bodies remain responsible for ensuring that appropriate procedures are put in place. Regarding group aspects, we refer in particular to Chapter A.	No change
Principle 20	Respondents suggested clarifying the exact scope of any new product approval policy (NPAP) (one single document vs. a set of rules, principles or committees that do not necessarily result in one single policy document). For the sake of completeness, it should be clarified what kind of products it refers to (products for clients – corporate,	As for the issue of one single document for NPAP vs. the possibility of having a set of policies, committees and documents, there is no need for one single document, but a set of procedures needs to be accessible and understandable in order to provide a clear and comprehensive new product approval policy.	No change

	retail, private, corresponding banking, etc.). If the principle refers to the entire set of policies, rules and committees related to new products, although not included in one single document, the gap would be relatively small. If, instead, Principle 20 refers to a sole comprehensive document covering all aspects (risk, commercial, reputational, tax, accounting, operational, etc) the gap is relatively large. Respondents assumed that this is not the spirit or intent of the principle.		
113	Respondents pointed out that it is not the task of a board of directors to approve new products and later changes. This should be left to the management body in its management function.	Principle 20 elaborates on the process and does not intend to shift the responsibility for such approvals to the supervisory function. In the quoted paragraph no reference is made to the supervisory function.	No change
D. Internal Control			
Principle 21	Respondents proposed including the three-lines-of-defence model in the Guideline to clarify the roles and interactions of the different functions.	The EBA is of the opinion that its Guideline is compatible with the three-lines-of-defence model, but EBA guidelines are not the right place for elaborating on this model in general.	No change
119	Respondents suggested that the report by the internal control function should be presented to the annual general meeting instead of to the management body.	Any management body needs to receive appropriate information on a regular basis to fulfil its duties. Shareholders and other stakeholders will receive information through the institutions' disclosure of risk related information as described in Chapter F of the Guidebook.	No change
119/120/	Respondents suggested that the internal control function should report to the	CP 44 uses management body as a concept. The control function should regularly report to the management body	No

122	management body in its management function instead of the management body in its supervisory function.	in its management function and, exceptionally, also to the management body in its supervisory function and/or the risk committee. The actual reporting lines to the supervisory function will differ depending on the governance structure and information required by the supervisory function. See also the comment for paragraph 78.	change
124	Participants commented that it is important to have an internal control function which forms a holistic view of all risks.	This is contained in paragraph 124 of the Guidebook.	No change
132	Respondents pointed out that the requirement that risk management must be consulted before the management body can make any decision would run contrary to any independent management of the institution by the management body. The management body has the decision making power. This would also give the management body the right to decide whether it wishes to consult risk management before making a decision or not. Regarding the example referring to changes to the senior management, it is not clear why any change to those responsible for human resources should have an impact on a bank's risk management.	CP 44 states that the risk control function (RCF) should be involved before material changes and exceptional transactions are decided. This is followed by a non-exhaustive list of possible examples for major changes. The paragraph was clarified. Decisions by management bodies would normally take evaluations performed by the RCF into account. Management bodies still can take decisions, without involving the RCF. Management bodies may also or evaluate the risks themselves. However, if major changes were regularly implemented without involving the RCF in risk assessments, this might be an indication that a management body had failed to implement a sound internal governance framework. The list of examples was amended.	Title II, 27.8 amended

136	Respondents were supportive of this guideline and suggested that the RCF should employ control cycle techniques here, by setting estimates, analysing actual outcomes against previous estimates, resetting estimates and repeating the cycle in each subsequent period.	Principle 23 describes the role of the risk control function. Analysis of trends and new emerging risks is an ongoing task of the RCF. This is already contained in the Guidebook. It was not intended to prescribe a specific procedure.	No change
137	Respondents commented that the review of the activities of subsidiaries and their compliance with approved group strategies should be a responsibility of internal audit rather than the risk control function.	While actual implementation is accomplished by group entities, group control functions oversee subsidiaries' control functions. The RCF also monitors the risks taken. At a later stage internal audit will check compliance with group policies as stated in Paragraph 154 of CP 44. The requirement was clarified.	Tirle II, 25.5 and 27.13 amended
Principle 24	As in smaller and less complex institutions this function would be performed by e.g. the finance director, respondents suggested changing Principle 24 as follows: "An institution should 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."	The principle of proportionality applies also to this principle. Thus it is possible for smaller and less complex institutions to assign the function to another person together with other tasks. Possible conflicts of interest need to be considered. This is already explained in Paragraph 146 of CP 44.	No change
Principle 24	Respondents stated that several conditions must be met (e.g. resources allocated, freedom to use resources as needed, a sound internal control system) to enable a CRO to effectively discharge his or her role. Responsibilities for those prerequisites need to be assigned to proper persons or bodies. Mechanisms are needed to attract and retain skilled people.	The Guideline (Principle 21, paragraph 119-122) already contains guidelines regarding the internal control function's resources, remuneration and access to information. Management bodies have the ultimate responsibility of ensuring that the necessary preconditions are met. Regarding remuneration, the EBA has published a separate guideline.	No change

144	Respondents pointed out that paragraph 144 intends to give CROs a right of veto over decision making, which would be incongruous with company law in some Member States. Company law contains the majority principle for decision making. It was suggested that CROs should have the right to contact the chairpersons of their boards.	A right of veto would be a possible way of strengthening the position of the CRO, which should be considered by institutions. That the CRO can approach the supervisory function directly, if needed, is already contained in the Guidebook. CP 44 did not intend to make a right of veto over decisions of management bodies mandatory. Implementation by institutions needs to be in line with applicable company law. How and on which level a possible right of veto would apply needs to be defined by each institution. See also paragraph 145 of CP 44. The language was clarified.	Title II, 28.3 amended
147	Respondents commented that CROs were being appointed by the Executive Management and therefore believed that the prior approval of the supervisory function on a replacement should not be necessary, while prior information should be mandatory.	If a CRO is a member of a management body different procedures will have to be followed, taking into account national company law. A CRO needs to have the appropriate standing and appropriate authority. The requirement that the supervisory function of a management body needs to approve the replacement of a CRO, aims at ensuring the appropriateness of the CRO's position, in particular in cases where he or she is not member of the management body.	No changes
Principle 25	Respondents pointed out that further discussion on the merits of the creation of a compliance function in credit institutions is needed; exemptions should be granted based on the principle of proportionality, especially for small institutions and subsidiaries which are already subject to a group compliance function. Other risk and control functions should be permitted to assist institutions in managing "compliance risk" for certain laws/regulations	The principle of proportionality applies to the Guidebook. While there may be no need in smaller institutions to have dedicated staff to perform the compliance function, the institution needs to exercise the respective tasks. Paragraph 119 of CP 44 states that the risk control and the compliance function can be combined. This has also been included in paragraph 149. The compliance function may delegate some tasks to specialised functions if specific input is needed, avoiding conflicts of interest.	Title II, 29.3 amended

	which are very specialised or technical (e.g. tax, labour and workplace health and safety law, accounting law, Basel II etc.).		
Principle 25	It should be possible to have several policies for managing compliance risk in each single matter of competence, instead of one single policy covering all compliance topics.	A compliance policy may consist of several chapters or documents, which can be considered as the compliance policy. It is important that the policy be approved and communicated to the staff. The latter must be done in such a way that all staff are informed about relevant policies.	No change
Principle 26	Respondents commented that internal audit is a key function in the internal governance framework and suggested elaborating more on this function in order to emphasise the following areas: independence, professionalism, mandate of audit, etc. in a separate chapter of the Guidebook.	Within the Guideline it was necessary to stress the importance of the internal audit function with regard to the assessment of the internal governance framework. The EBA does not intend to develop a full set of internal audit guidelines in parallel to the generally accepted standards available.	No change
Principle 27	Respondents suggested that audit plans should also be prepared based on the results of the risk assessment process on the main elements of the audit universe. Boards of directors should approve the annual audit plans and any relevant changes to them.	Paragraph 156 of CP 44 recommends adhering to national or international professional standards. The EBA agrees that audits should be performed using a risk-based approach and that an audit plan should be approved by the management body and audit committee. The latter was clarified in the Guidelines.	Title II, 30.5 amended
E. Information system and business continuity			
160	Respondents requested that paragraph 160 should make it clear that the internal audit function may provide independent monitoring of information systems with or without	There seems to be no reason to clarify the wording since outsourcing issues are addressed elsewhere in the document.	No change

	externally sourced assistance.		
162	Respondents requested that "enable" be replaced with "contribute" in paragraph 162 ("The results of the analysis should enable an institution to define its recovery priorities and objectives")	The comment has been accommodated.	Title II, 32.2 amended
F. Transparency			
Principle 29, 166-167	Respondents commented that not all staff members need to be informed about high-level strategies/detailed business strategies (as they may be confidential and possess proprietary value).	Following the comment, paragraph 167 was changed to "update the relevant staff" to indicate that only relevant staff members need to be informed. Information needs to be provided in a clear and consistent way. Furthermore, paragraph 167 already refers to strategies and policies which are subject to internal communication ("...at least to the level needed to carry out their particular duties."). Paragraph 166 and the principle itself contain similar references; therefore no further change was needed.	Title II, 33.3 amended
Principle 30	Respondents requested that a reference to the need to consider competitive and legal concerns ("taking into account appropriate competitive and legal considerations of the institution") be added.	Since legal aspects have to be considered anyway there is no need to mention them explicitly here. Institutions need to find the right balance between providing sufficient information on their governance and current positions and taking care of confidentiality aspects. This is already possible under the current wording.	No change
168	Respondents asked to add "employees and employment committees" to the list of stakeholders provided.	The list is non comprehensive; "employees" has been added to the list of examples.	Title II, 34.1 text in box amended

169	Participants in the public hearing commented that the transparency requirements (information about internal governance) at group and individual level were difficult to meet, in particular in large groups. It would be sufficient to ask for transparency at group level only.	This comment has been accommodated and now follows the approach used in Article 72 of the CRD regarding Pillar 3 disclosures (even though is not clear from the text of the CRD (Annex XII) that internal governance disclosure as such falls under Pillar 3 requirements). However, it is good practice for every institution to disclose information on its internal governance in a proportionate way to inform local stakeholders.	Title II, 34.1, text in box amended
170	Respondents requested that "explanation of how they could influence the entire organisation "be deleted, as this cannot be predicted. Moreover, it was not entirely clear to participants what „influences the entire organisation" meant.	This comment has been accommodated in order to clarify the issue and paragraph 170 was amended as follows: "… the nature, extent, purpose and economic substance of transactions with affiliates and related parties, if they have a material impact on the institution;".	Title II, 34.2 amended.