13 October 2010

Consultation paper on the Guidebook on Internal Governance (CP 44)

Table of contents

Overview

1. Importance of internal governance

1. 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.

2. In recent years, internal governance issues have received more and more attention from various international bodies[1]. Their main effort has been to correct 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.

3. In late 2009, CEBS undertook a **survey on the implementation** by supervisory authorities and institutions of its **Internal Governance Guidelines** published in January 2006[2]. The survey's main results[3] were that, although overall the regulatory and supervisory national frameworks for internal governance could be considered broadly complete, their coverage was somewhat fragmented, with a number of gaps identified. The survey also revealed that institutions needed to improve their implementation of the Guidelines and supervisors to enhance their procedures regarding this matter.

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

---

[1] 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

[2] They are included in the Guidelines on the Application of the Supervisory Review Process under Pillar 2 and are available under the following link: http://www.c-ebs.org/getdoc/00ec6db3-bb41-467c-acb9-8e271f617675/GL03.aspx

[3] See a summary of the results under the following link: http://www.c-ebs.org/documents/About-us/Key-dates/Summary-of-survey-results_Workshop-on-Internal-Gov.aspx

sufficiently 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 not always transparent and organised in a way that promoted and demonstrated effective and prudent management, often because of ineffective reporting lines.

5. 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 fulfill their duties.

6. 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 on all risks did not exist. Control functions often lacked appropriate standing, in terms of resources, status and/or expertise.

7. 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, 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 Guidebook on Internal Governance

8. CEBS has already addressed some of the most significant issues arising from the financial crisis within its **High Level Principles on Remuneration**[4] published in April 2009 and in its **High Level Principles on Risk Management**[5] published in February 2010. However, taking into account the findings of the CEBS's 2009 survey and the recent work by other European and international bodies on corporate governance (especially the Basel Committee's Principles for enhancing corporate governance), CEBS saw merit in enhancing these High Level Principles. Accordingly, CEBS decided to add guidelines concerning the functioning

[4] See: http://www.c-ebs.org/getdoc/34beb2e0-bdff-4b8e-979a-5115a482a7ba/High-level-principles-for-remuneration-policies.aspx

[5] See: http://www.c-ebs.org/documents/Publications/Standards---Guidelines/2010/Risk-management/HighLevelprinciplesonriskmanagement.aspx

and composition of the management body as well as the qualification, appointment and succession of its members and to improve the principles dealing with the Risk Control function.

9. CEBS has consolidated all of its guidelines specifically aimed at internal governance in the present Guidebook on Internal Governance (the "**Guidebook**"). CEBS's Internal Governance Guidelines have been reviewed and merged with the High Level Principles on Remuneration and on Risk Management. The Guidebook unifies the concepts used, sets those High Level Principles in the context of internal governance and takes into account the weaknesses identified in the survey and developments since the publication of the Guidelines on the Supervisory Review Process in 2006 (e.g. group context, systems and continuity).

10. The focus of the Guidebook is limited to internal governance and so excludes other aspects of corporate governance (see "Section 3. Concepts used in the Guidebook" below). It does therefore not cover the roles of external auditors, shareholders or other external stakeholders.

11. 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 Guidebook, which is limited to Principles directly aimed at the sound implementation of internal governance in institutions.[6] All Guidelines published by CEBS can be accessed via CEBS's website[7].

3. Concepts used in the Guidebook

12. **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.

[6] These guidelines are also not concerned with internal provisions that apply to investment services and that are included in the MIFID.

[7] See : http://www.c-ebs.org/Publications/Standards-Guidelines.aspx

13. **Internal governance** for institutions[8] in the European Community is codified in **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, and adequate internal control mechanisms, including sound administrative and accounting procedures".

14. 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.

15. CEBS is aware that within 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 Principle 6.

16. The Guidebook does not advocate any particular structure. The term '**Management body**' is used in the Guidebook to embrace both 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 Guidebook generally does 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 crux is that the task or responsibility is fulfilled.

---

[8] Institutions referred to in this guidebook are credit institutions and investment firms to which 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 CRD is available at: http://ec.europa.eu/internal_market/bank/regcapital/index_en.htm

17. 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**.

18. An institution should also 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.

19. In assessing the efficiency of Internal Control within an institution, the management body should 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.

20. **"Risk tolerance/appetite"** is used to embrace all relevant definitions used by different institutions and supervisory authorities. While some use "risk tolerance" to describe the amount of risk an institution is willing to accept, others use "risk appetite" to distinguish between the absolute risks an institution *a priori* is open to take (risk appetite) and the actual limits within its risk appetite an institution pursues (risk tolerance).

4. Implementation of the Guidebook

21. **The Guidebook aims to harmonise supervisory expectations** and to improve the sound implementation of internal governance arrangements, especially of large and complex institutions. Therefore, the Principles contained in the Guidebook should be considered both by institutions and supervisors within the supervisory review framework under Pillar 2. Accordingly they should be implemented by institutions as part of their Internal Capital Adequacy Assessment Process ("**ICAAP"**) and reviewed by supervisors as part of their Supervisory Review and Evaluation Process ("**SREP**"). By enhancing the implementation of their internal governance framework, institutions will become more resilient against adverse market conditions and will accordingly contribute to the stability of the financial sector.

22. It is important to note that **proportionality**, as laid down in the CRD, applies to all guidelines contained in the Guidebook. An institution may demonstrate how its approach, reflecting the nature, scale and complexity

of its activities, meets the outcome required by the Guidebook, i.e. there is no "one size fits all" approach.

23. With the adoption and publication of the Guidebook, section 2.1 in the “Guidelines on Internal Governance” in the Guidelines on the Application of the Supervisory Review Process; the “High Level Principles on Remuneration” and the “High Level Principles for Risk Management” will be overridden.

24. CEBS expects its members to **implement** the Guidebook on Internal Governance and incorporate it within their supervisory procedures by 30. September 2011. After that date, members should ensure that institutions comply with it effectively.

A. Corporate Structure and Organisation

Principle 1 - Organisational framework

The management body should ensure a suitable and transparent corporate structure for an institution. The structure should 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 should be clear, well-defined, coherent and enforced.

25. The management body should ensure that the structure of an institution and, where applicable, the structures and reporting lines within a group are clear and transparent, both to the institution's own staff and to its supervisors.

26. 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 group faces.

27. The management body should assess how changes to the group's structure impact on its soundness. 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. The management body should make any necessary adjustments swiftly.

Principle 2 - Checks and balances in a group structure

In a group structure, the management body of an institution's parent company has the overall responsibility for adequate internal governance across the group and ensuring that there is a governance framework appropriate to the structure, business and risks of the group and its component entities.

28. The management body of a regulated subsidiary 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. However, the group dimension is likely to affect the internal governance structure of both the parent company and its subsidiaries. Their management bodies should

consider how to apply the Principles and take into account the paragraphs below.

29. 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 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.

30. In order to fulfil its internal governance responsibilities, the management body of an institution's parent company should:

- 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;
- approve an internal governance policy at the group level for its subsidiaries, which includes the commitment to meet all applicable governance requirements;
- ensure that enough resources are available for each subsidiary to meet both group standards and local governance standards; and
- have appropriate means to monitor that each subsidiary complies with all applicable internal governance requirements.

31. Reporting lines in a group should be clear and transparent, especially where business lines do not match the legal structure of the group.

32. The management body of a regulated subsidiary has its own internal governance responsibilities, should set its own 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:

- the sound and prudent management of the subsidiary;
- the financial health of the subsidiary; or
- the legal interests of the subsidiary's stakeholders.

33. In a subsidiary, an element of strong governance is to have independent members on the management body (e.g. non-executives who

are independent of the subsidiary and of its group, and of the controlling shareholder).

Principle 3 - Know-your-structure

The management body should 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.

34. 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.

35. 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.

36. 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 between 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.

37. 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.

38. 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 information on major risk drivers. To achieve this, regular reports are needed assessing the institution's overall structure and

evaluating individual entities' activities compliance with the approved strategy.

Principle 4 - Non-standard or non-transparent activities

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 should understand their purpose and structure and the particular risks associated with them. The management body should only accept these activities when it has satisfied itself the risks will be appropriately managed. [9]

39. 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 from conducting appropriate business oversight and hinder effective banking supervision. They should therefore only be approved and maintained when their purpose has been defined and understood, effective oversight has been ensured and all material associated risks they could generate can be appropriately managed.

40. 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. It should also maintain and review, on an on-going basis, appropriate strategies and policies governing the approval and maintenance of such structures and activities in order to ensure they remain consistent with their intended aim. All these structures and activities should be subject to periodic internal and external audit reviews.

[9] In addition to that principle, supervisory 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.

41. The management body should ensure appropriate actions are taken to avoid or mitigate all these challenges and the institution has adequate policies and procedures to:

- establish 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;
- ensure that 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;
- periodically assess the continuing need to perform activities that impede transparency.

42. The same measures should be taken when an institution performs certain activities for clients (e.g. helping clients form vehicles in offshore jurisdictions; developing complex structures and finance transactions for them or providing trustee services) since they pose similar internal governance challenges.

B. Management body

Principle 5 - Responsibilities of the management body

The management body has overall responsibility for the institution and should set the institution's strategy and risk appetite. The responsibilities of the management body should be clearly defined and approved.

43. The responsibilities of the management body are the basis for the sound and prudent management of the institution and should be defined in a written document.

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

- 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;
- the overall risk strategy and policy of the institution , including its risk tolerance/appetite and its risk management framework;

- the amounts, types and distribution of both internal capital and own funds adequate to cover the risks of the institution;
- a robust and transparent organisational structure with effective communication and reporting channels;
- a policy on the nomination and succession of individuals with key functions in the institution;
- a remuneration framework that is in line with the risk strategies of the institution;
- the governance principles and corporate values of the institution, including through a code of conduct or comparable document; and
- 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.

45. 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.

Principle 6 - Management and supervisory functions

The management body of an institution has two key functions: the management and supervisory function. These functions should interact effectively.

46. 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.

47. 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.

48. The supervisory function oversees the management function and provides advice to it. Its oversight role comprises of constructive challenge to develop 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. The management body in its supervisory function should:

- 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;
- 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
- monitor the performance of the members of the management body in its management function against those standards.

49. 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.

50. Effective interaction should mean the management body in its management function co-ordinating the institution's business and risk strategies with the management body in its supervisory function and discussing regularly the implementation of these strategies with the management body in its supervisory function.

51. 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.

Principle 7 - Composition, appointment and succession

The management body should have an adequate number of members and an appropriate composition. The management body should have policies for selecting, monitoring and planning the succession of its members.

52. 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.

53. 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.

54. 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. Members of the management body should be appointed for an appropriate period. 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.

55. 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.

Principle 8 - Commitment, independence and managing conflicts of interest

Members of the management body should engage actively in the business of an institution and should be able to make their own sound, objective and independent decisions and judgments.

56. The selection of members of the management body should ensure 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.

57. 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.

58. 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.

59. The members of the management body should be able to act critically and independently. The ability to exercise objective and independent judgment can be enhanced by recruiting members from a sufficiently broad population of candidates. Independence can be further enhanced by having sufficient non-executive members. Where the management body in its supervisory function is formally separate from the management body in its management function, objectivity and independence still need to be assured by appropriate selection of independent members.

60. The management body should have a written policy on managing conflicts of interests for its members. The policy should specify:

- a member's duty to avoid, to the extent possible, activities that could create conflicts of interest or the appearance of conflicts of interest;
- 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;
- a member's duty to inform the institution of any matter that may result, or has already resulted, in a conflict of interest;
- 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;
- adequate procedures for transactions with related parties to be made on an arms-length basis; and
- the way in which the management body would deal with any non-compliance with the policy.

Principle 9 - Qualifications

Members of the management body should be and remain qualified, including through training, for their positions. They should have a clear understanding of their institution's governance arrangements and their role in them.

61. The members of the management body, both individually and collectively, should have the necessary expertise, experience, competencies and personal qualities, including professionalism and personal integrity, to properly carry out their duties.

62. Members of the management body should have a level of up-to-date understanding commensurate with their responsibilities. This includes appropriate understanding of those areas for which they are not directly responsible but are collectively accountable.

63. 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.

64. There should be a sound process in place to ensure that the management body members, individually and collectively, have sufficient qualifications.

65. Members of the management body need to 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.

Principle 10 - Organisational functioning

The management body should 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.

66. 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.

67. 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

68. 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

69. 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.

70. 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.

71. 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, it is important for the institution to have measures in place to minimise the potential detriment on its checks and balances (for example, by having a lead senior independent member of the management body in its supervisory function or similar position).

Specialised committees

72. 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). 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. 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.

73. 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 to avoid undue concentration of power and to promote fresh perspectives. An institution should disclose its established committees and their mandates and composition.

74. 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

75. An audit committee[10] (or equivalent) should oversee the institution's internal and 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.

76. 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.

[10] See also Art 41 of Directive 2006/43/EC on statuary audits of annual accounts an consolidated accounts, accessible under the following link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0087:0107:EN:PDF

77. 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

78. A risk committee (or equivalent) could 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.

Principle 11 - Corporate values and code of conduct

The management body should develop and promote high ethical and professional standards.

79. 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.

80. 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 risk will be reduced if these standards are given high priority and implemented soundly. The management body should therefore have clear policies for how these standards should be met and should perform a continuing review of their implementation.

Principle 12 - Conflicts of interest at institution level

The management body should establish, implement and maintain effective policies to identify actual and potential conflicts of interest so they can be prevented. If conflicts of interest cannot be prevented, they should be appropriately managed.

81. A written policy should identify the relationships, services, activities or transactions of an institution in which conflicts of interest may arise and how these conflicts should be managed. Relationships and transactions which may create conflicts of interest include those between different clients of an institution and those between an institution and:

- its customers (as a result of the commercial model and/or the various services and activities provided by the institution);
- its shareholders;
- the members of its management body;
- its staff; and
- other related institutions (e.g. its parent company or subsidiaries).

82. A parent company should consider and balance the interests of all its subsidiaries, how these interests contribute to the common purpose and interests of the group as a whole over the long term.

83. The conflict of interest policy should set out measures to be adopted to prevent or manage conflicts of interest (see also under Principle 8). Such procedures and measures might include:

- 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;
- establishing information barriers such as physical separation of certain departments; and
- preventing people who are also active outside the institution from having inappropriate influence within the institution regarding those activities.

Principle 13 - Internal alert procedures

The management body should put in place appropriate internal alert procedures for communicating internal governance concerns from the staff.

84. 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 raise such concerns.

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

85. 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.

Principle 14 - Outsourcing

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

86. 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.

87. 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.

88. 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.

89. Institutions are referred to the CEBS Guidelines on Outsourcing for details on this principle.[11]

[11] The Guidelines on Outsourcing are available at: http://www.c-ebs.org/getdoc/f99a6113-02ea-4028-8737-1cdb33624840/GL02OutsourcingGuidelines-pdf.aspx

Principle 15 - Governance of remuneration policy

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

90. The management body in its supervisory function should maintain, approve and oversee the principles of the overall remuneration policy for its institution (as discussed below in Principle 18). The institution's procedures for determining remuneration should be clear, well documented and internally transparent.

91. 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 judgment on the suitability of the remuneration policy, including its implications for risk management.

92. 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.

93. 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.

94. For details on this principle, institutions are referred to the Guidelines on Remuneration[12] that CEBS has issued following the CRD remuneration requirements and to all further references included in those guidelines (such as the FSB Principles and Implementation Standards).

[12] The Guidelines can be found under the following link: http://www.c-ebs.org/Publications/Standards-Guidelines.aspx

Principle 16 - Assessment of the internal governance framework

The management body should monitor and periodically assess the effectiveness of the institution's internal governance framework.

95. 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.

C. Risk management

Principle 17- Risk culture

An institution should 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.

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

97. 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.

98. 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.

99. 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.

100. The risk management framework should be subject to independent 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 like 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.

Principle 18 - Alignment of remuneration with risk profile

An institution's remuneration policy and practices should be consistent with its risk profile and promote sound and effective risk management.

101. 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.

102. For staff whose responsibilities 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), the remuneration policy should set up specific arrangements to ensure their remuneration is aligned with sound and effective risk management.

103. 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.

104. 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 risk and the cost of capital.

105. 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.

106. For details on this principle, institutions are referred to the Guidelines on Remuneration that CEBS has issued following the CRD remuneration requirements, and to all further references included in those guidelines (such as the FSB Principles and Implementation Standards).

Principle 19 - Risk management framework

An institution's risk management framework should 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.

107. 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.

108. When identifying and measuring risks, an institution should develop forward-looking and backward-looking tools to complement work on current exposures. Forward-looking tools (such as scenario analysis and stress tests[13]) 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. The tools should allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations.

109. External risk assessments (including external credit ratings or externally purchased risk models) can help provide a more comprehensive estimate of risk. However 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[14].

110. Decisions which determine the level of risks taken should not only be based on quantitative information or model outputs but should also take into account the practical and conceptual limitations of metrics and models, using a qualitative approach (including expert judgment and critical

[13] The Stress test guidelines can be found under the following link: http://www.c-ebs.org/documents/Publications/Standards---Guidelines/2010/Stress-testing-guidelines/ST_Guidelines.aspx

[14] 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.

analysis). Relevant macroeconomic environment trends and data should explicitly be addressed to identify their potential impact on exposures and portfolios. Such assessments should be formally integrated into material risk decisions. In particular, an institution should bear in mind that the results of 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.

111. 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. Regular and transparent reporting mechanisms should be established so 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.

112. 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.

Principle 20 - New products

An institution should 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.

113. 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.

114. 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.

115. 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

Principle 21 - Internal control framework

An institution should develop and maintain a strong and comprehensive internal control framework, including specific independent control functions with appropriate standing to fulfil their mission.

116. 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.

117. 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.

118. 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.

119. 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.

120. A control function can generally be regarded as independent if:

- its staff do not perform any tasks that fall within the scope of the activities the control function is intended to monitor and control;
- it is organisationally separate from the activities it is assigned to monitor and control;
- 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
- 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.

121. 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, including through 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.

122. 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.

Principle 22 - Risk Control function

An institution should establish a comprehensive and independent Risk Control function ("RCF").

123. 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 could accomplish this by providing 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 can recommend improvements to the risk management framework and options to remedy breaches of risk policies, procedures and limits.

124. 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.

125. 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 bear responsibility for managing risk.

Principle 23 – The Risk Control function's role

The RCF should be actively involved at an early stage in elaborating an institution's risk strategy and in all material risk management

decisions. The RCF should play a key role in ensuring the institution has effective risk management processes in place.

Strategy and decisions

126. 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.

127. 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.

128. The RCF shares responsibility for implementing an institution's risk strategy and policy with all the institution's business units. While the business units implement the relevant risk limits, the RCF is 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's is not taking on excessive risk.

129. The RCF's involvement in the decision-making processes should ensure risk considerations are taken into account appropriately. However, accountability for the decisions taken remains with the business and support units and ultimately the management body.

Transactions with related parties

130. 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.

Complexity of the legal structure

131. The RCF should help to identify material risks arising from the complexity of an institution's legal structure. Risks may include a lack of management transparency, operational risks introduced by inter-connected and complex funding structures, intra-group exposures, trapped collateral and counterparty risk. 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.

Material changes

132. Before any decision is taken, the RCF should evaluate the impact of material changes and exceptional transactions on the institution's and group's overall risk profile. These might include mergers and acquisitions[15], creation or sale of subsidiaries or SPVs, new products, changes to systems, risk management framework or procedures and changes to the institution's organisation or senior management.

133. Changes to the group structure (including merger and acquisitions) can pose special risk management challenges. The RCF should be actively involved at an early stage in identifying relevant risks related to these operations (including potential consequences from conducting insufficient due diligence that fails to identify post-merger risks) and should report its findings directly to the management body.

Measurement and assessment

134. The RCF should ensure that an institution's internal risk measurements and assessments cover an appropriate range of scenarios and are not based on overly optimistic assumptions regarding dependencies and correlations. This should include qualitative (including with expert judgment) firm-wide views on the relationships between the risks and profitability of the institution and its external operating environment.

Monitoring

135. 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.

---

[15] See the three Level-3 Committees of European Financial Supervisors (CEBS, CESR, and CEIOPS) joint guidelines on the prudential assessment of acquisitions and increases in holdings in the financial sector: http://www.c-ebs.org/getdoc/09acbe4b-c2ee-4e65-b461-331a7176ac50/2008-18-12_M-A-Guidelines.aspx

136. 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.

137. The Group RCF should review the consistency of the activities of subsidiaries with approved group strategy and report its findings to the management body.

Unapproved exposures

138. The RCF should be adequately involved in any changes to the institution's strategy, approved risk tolerance/appetite and limits.

139. 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.

140. 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.

141. 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.

142. 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)[16].

[16] 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).

Principle 24 - Chief Risk Officer

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.

143. The CRO (or equivalent position) is responsible for providing comprehensive, understandable and well interpreted 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 group.

144. The CRO should have sufficient expertise, operating experience, independence and seniority to challenge (and potentially veto) decisions that affect an institution's exposure to risk. The CRO and the management body or relevant committees should be able to communicate directly amongst themselves on key risk issues including developments that may be inconsistent with the institution's risk tolerance/appetite and strategy.

145. 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.

146. 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.

147. 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.

Principle 25 - Compliance function

An institution should have a compliance policy and establish a Compliance function to manage its compliance risk.

148. 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. Accordingly, an institution should approve and implement a compliance policy which should be communicated to all staff.

149. 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).

150. The Compliance function should ensure that the compliance policy is observed and report to the management body on the institution's management of compliance risk. The findings of the Compliance function should be taken into account by the RCF within the decision-making process.

151. 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.

152. 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. 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.

Principle 26 - Internal Audit function

The Internal Audit function ("IAF") should assess whether the quality of an institution's internal control framework is both effective and efficient.

153. The IAF is responsible for assessing the adequacy of an institution's internal control framework. To do this, the IAF should have unfettered access to relevant documents and information in all operational and control units.

154. 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.

155. The IAF should assess, in particular, the adequacy and 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.

156. The management body should encourage the internal auditors to adhere to national and international professional standards[17]. Internal audit work should be performed in accordance with a strategic audit plan and detailed audit programs following a "risk based" approach.

157. 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. Systems and continuity

Principle 27 - Information system and communication

An institution should have effective and reliable information and communication systems covering all its significant activities.

158. 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.

159. 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.

[17] Such as those established by the Institute of Internal Auditors.

160. 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 consider generally accepted IT Standards when implementing IT systems.

Principle 28 - Business continuity management

An institution should establish a sound business continuity management to ensure its ability to operate on an on-going basis and limit losses in the event of severe business disruption.

161. 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.

162. By taking into account external data and performing scenario analysis, an institution should carefully analyse its exposure to severe business disruptions and assess (quantitatively and qualitatively) their impact. 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[18] should be actively involved. The results of the analysis should enable an institution to define its recovery priorities and objectives.

163. Contingency and business continuity plans should be in place 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.

164. An institution should have recovery plans for critical resources in place 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.

[18] See Directive 2006/48/EC Annex X, Part 3, Par. 4 which requires for AMA-institutions an Operational Risk Management function; the tasks of this function are described in the Guidelines on Validation par. 615-620 (published 2006) which is available at: http://www.c-ebs.org/documents/Publications/Standards---Guidelines/2010/Stress-testing-guidelines/ST_Guidelines.aspx.

165. 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

Principle 29 - Empowerment

Strategies and policies should be communicated to all relevant staff throughout an institution.

166. An institution's staff should understand and adhere to policies and procedures pertaining to their duties and responsibilities.

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

Principle 30 - Internal governance transparency

The internal governance framework of an institution should be transparent. An institution should present its current position and future prospects in a clear, balanced, accurate and timely way.

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

169. An institution should disclose comprehensive and meaningful information that fully describes its internal governance at group and solo levels.

170. An institution should publicly disclose at least the following:

- 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;
- the nature, extent, purpose and economic substance of transactions with affiliates and related parties and an explanation of how they could influence the entire organisation;
- how its business and risk strategy is set (including the involvement of the management body) and foreseeable risk factors;
- 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
- material information about its financial and operating results;

171. Information about the current position of the institution should comply with any legal disclosure requirements. Information should be clear, accurate, relevant, timely and accessible.

172. In cases where ensuring a high degree of accuracy would delay the release of time-sensitive information, an institution should make a judgment 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.