APPENDIX 1

PRINCIPLES ON INTERNAL GOVERNANCE

Title I - Subject Matter and Scope

1. Subject Matter

The Principles aim to harmonise supervisory expectations and to improve the sound implementation of internal governance arrangements in line with, *inter alia*, the Banking Act (the Act) Section 17B, Annex 2B of this Rule and the Companies Act *Cap. 386*.

2. Scope and level of application

1. The Authority shall require institutions to comply with the provisions laid down in these Principles on Internal Governance.

2. The application of these Principles shall be reviewed by the Authority as part of its Supervisory Review and Evaluation Process.

> Explanatory note
>
> CEBS/EBA had drawn up Guidelines on the Supervisory Review Process, which can be found on the EBA website (http://www.eba.europa.eu/getdoc/00ec6db3-bb41-467c-acb9-8e271f617675/GL03.aspx).

3. The Principles 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 paragraph 12 of this Rule, applies to all provisions contained in the Principles. An institution may be required to demonstrate how its approach, reflecting the nature, scale and complexity of its activities, meets the outcome required by the Principles.

Title II – Requirements Regarding Institutions' Internal Governance

A. Corporate Structure and Organisation

3. Organisational Framework

1. The Board of Directors 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 Board of Directors 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 Board of Directors 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 Board of Directors to oversee and manage effectively the risks the institution or the group faces.

4. The Board of Directors should assess how changes to the group's structure impact on its soundness. The Board of Directors should be in a position to make any necessary adjustments swiftly.

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

4. Checks and balances in a group structure

1. In a group structure, the Board of Directors 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 Board of Directors 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 Board of Directors 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 subsidiary in breach of applicable legal or regulatory provisions or prudential rules. The Board of Directors 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 Boards of Directors 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 Board of Directors 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' Board of Directors.

5. In order to fulfil its internal governance responsibilities, the Board of Directors 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 Board of Directors. Independent members of the Board of Directors are non-executive directors who are independent of the subsidiary and of its group, and of the controlling shareholder.

5. Know-your-structure

1. The Board of Directors 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 Board of Directors 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 Board of Directors 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 Board of Directors 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 Board of Directors 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 Board of Directors 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 Board of Directors, the control functions and supervisors, as appropriate.

5. The Board of Directors 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' compliance with the approved strategy.

6. Non-standard or non-transparent activities

1. Without prejudice to the provisions of Article 11(3) of the Act, where an institution operates through special-purpose or related structures or in jurisdictions that impede transparency or do not meet international banking standards, the Board of Directors shall understand their purpose and structure and the particular risks associated with them. The Board of Directors shall only accept these activities when it has satisfied itself the risks will be appropriately managed.

Explanatory note

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. These jurisdictions may also impede the ability of the Board of Directors to conduct appropriate business oversight and hinder effective banking supervision. Operations in such jurisdictions 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 risks associated with these structures can be appropriately managed and as stated above, subject to the provisions of Article 11(3) of the Act.

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

2. The Board of Directors 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 Board of Directors 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 Board of Directors and if and where necessary, to the Authority;

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. Board of Directors

B.1 Duties and responsibilities of the Board of Directors

7. Responsibilities of the Board of Directors

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

Explanatory note The sound execution of the responsibilities of the Board of Directors is the basis for the sound and prudent management of the institution. The documented responsibilities have also to be in line with the Companies' Act 1986 and with any other national company laws in jurisdictions where the institution may be established.

2. The key responsibilities of the Board of Directors 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 Board of Directors should also regularly review and adjust these policies and strategies. The Board of Directors is responsible for appropriate communication with the Authority and other interested parties.

8. Assessment of the internal governance framework

1. The Board of Directors 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.

9. Management and supervisory functions of the Board of Directors

1. The Board of Directors of an institution shall interact effectively with senior management.

2. The Board of Directors should:

a. be ready and able to challenge and review critically in a constructive manner propositions, explanations and information provided by members of the senior management;

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 senior management against those standards.

3. The senior management should coordinate the Institution's business and risk strategies with the Board of Directors and discuss regularly the implementation of these strategies with the Board of Directors.

4. The Board of Directors and senior management should provide each other with sufficient information. The senior management should comprehensively inform regularly, and without delay if necessary, the Board of Directors 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 Board of Directors

10. Composition, appointment and succession of the Board of Directors

1. The Board of Directors shall have an adequate number of members and an appropriate composition. The Board of Directors shall have policies for selecting, monitoring and planning the succession of its members.

2. An institution should set the size and composition of its Board of Directors,taking into account the size and complexity of the institution and the nature and scope of its activities. The selection of members of the Board of Directors should ensure sufficient collective expertise.

3. The Board of Directors should identify and select qualified and experienced candidates and ensure appropriate succession planning for the Board of Directors and senior management, giving due consideration to any other legal requirements regarding composition, appointment or succession.

4. The Board of Directors 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 Board of Directors 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 Board of Directors should consider the expiry date of each member's contract or mandate to prevent, where possible, too many members having to be replaced simultaneously.

11. Commitment, independence and managing conflicts of interest in the Board of Directors

1. Members of the Board of Directors 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 Board of Directors should ensure that there is sufficient expertise and independence within the Board of Directors . An institution should ensure that members of the Board of Directors are able to commit enough time and effort to fulfil their responsibilities effectively.

3. Members of the Board of Directors 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 Board of Directors 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 Board of Directors should challenge how that individual will spend sufficient time fulfilling his/her responsibilities towards the institution. Attendance of the members of the Board of Directors should be disclosed. An institution should also consider disclosing the long-term absence of members of the senior management.

5. The members of the Board of Directors should be able to act objectively, critically and independently. Measures 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.

6. The Board of Directors 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 Board of Directors , 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 company's or institution's Board of Directors) 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 Board of Directors would deal with any non-compliance with the policy.

12. Qualifications of the Board of Directors and senior management

1. Members of the Board of Directors and senior management 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 Board of Directors and senior management, 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 Board of Directors and senior management 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 Board of Directors and senior management members, individually and collectively, have sufficient qualifications.

6. Members of the Board of Directors and senior management hould 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 that individual members are not directly responsibility for. The Board of Directors and senior management should ensure that the institution dedicates sufficient time, budget and other resources to training of personnel.

13. Organisational functioning of the Board of Directors

1. The Board of Directors 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 Board of Directors 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 Board of Directors should meet regularly in order to carry out its responsibilities adequately and effectively. The members of the Board of Directors 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 Board of Directors, should be documented and periodically reviewed by the Board of Directors.

Assessment of the functioning of the Board of Directors

3. The Board of Directors 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 Board of Directors

4. The Chair should ensure that Board of Directors' 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 Board of Directors plays a crucial role in the proper functioning of the Board of Directors. He or she provides leadership to the Board of Directors and is responsible for its effective overall functioning.

5. The Chair of the Board of Directors and the Chief Executive Officer of an institution should not be the same person.

Specialised committees of the Board of Directors

6. The Board of Directors should consider, taking into account the size and complexity of an institution, setting up specialized committees consisting of members of the Board of Directors and (where appropriate), senior management (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 Board of Directors from collectively discharging its duties and responsibilities but can help support the Board 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 Board of Directors and established working procedures. An institution may consider occasionally rotating membership and chairmanship of a committee.

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 Board of Directors. 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 Board of Directors the appointment, compensation and dismissal of the external auditors; review and approve the audit scope and frequency; review audit reports; and check that senior management 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.

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 banking and/or 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 Board of Directors 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

14. Corporate values and code of conduct

1. The Board of Directors 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 Board of Directors should set clear policies for how these self-imposed 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 Board of Directors on a regular basis.

15. Conflicts of interest at institution level

1. The Board of Directors 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 Board of Directors 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 Board of Directors ;
   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 policy on conflict of interest 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.

16. Internal alert procedures

1. The Board of Directors shall put in place appropriate internal alert procedures for communicating internal governance concerns from the staff ('whistle-blowing').

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 institution's Compliance function or the Internal Audit function or an internal 'whistle-blower' procedure if such procedure is in place. 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 Board of Directors.

B.4 Outsourcing and remuneration policies

17. Outsourcing

1. The Board of Directors and Senior Management shall approve and regularly review the outsourcing policy of an institution.

Explanatory note The above Principle is limited to the outsourcing policy, as specific aspects of the issue of outsourcing are treated in Banking Rule BR/14. Institutions are expected to comply with this Principle as well as the provisions of Banking Rule BR/14. In case of any discrepancies, Banking Rule BR/14 shall prevail, as it is more specific. In case an issue is not covered by the provisions of Banking Rule BR/14, the general Principle above 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 any 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.

18. Governance of remuneration policy

1. Ultimate oversight of the remuneration policy shall rest with an institution's Board of Directors.

Explanatory note The above Principle provides the general framework applicable to the governance of the remuneration policy. Specific aspects of the issue of remuneration are treated in Annex 2E of this Banking Rule, which reflect the CEBS Guidelines. Institutions are expected to comply with this Principle as well as with Annex 2E.

2. The Board of Directors 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 Board of Directors' general responsibility for the overall remuneration policy and its review, adequate involvement of the control functions is required. Members of the Board of Directors, 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. Senior Management 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 Board of Directors 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

19. 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, which effectively are under the oversight of the Board of Directors and an institution's Senior Management, 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 set 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.

20. 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 above Principle provides 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 Annex 2E. Institutions are expected to comply with this Principle as well as with Annex 2E of this Rule.

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. Board of Directors, 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.

21. 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 principles can be found in Annex 2D of this Banking Rule.

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 Board of Directors, Senior Management 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 Board of Directors.

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.

22. New products

1. An institution shall have in place a well-documented new product approval policy ('NPAP'), approved by the Board of Directors, 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

23. 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 Board of Directors. 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 that the control function monitors and controls. The head of the control function generally should report directly to the Board of Directors 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 that 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 Board of Directors 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 Board of Directors should act on the findings of the control functions in a timely and effective manner and require adequate remedial action.

24. 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 Board of Directors . The RCF should provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by the Board of Directors, senior management 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.

25. 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 Board of Directors 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 Board of Directors 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 that the limits are in line with the institution's overall risk appetite/risk tolerance and monitoring on an on-going basis in order to ensure 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 Board of Directors.

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, that they pose for the institution are identified and adequately assessed.

RCF's role in the 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 Board of Directors.

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 institution's Senior Management and challenge by the Board of Directors.

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 Board of Directors.

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 Board of Directors, Senior Management, 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 principles 'fraud' encompasses internal and external fraud as defined in, *inter alia*, Banking Rule BR/04 Appendix 4 Section I.6. 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).

26. 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 Board of Directors 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 Board of Directors 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 under which 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 Board of Directors 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 Board of Directors. Generally the removal or appointment of a CRO should be disclosed and the Authority informed about the reasons.

27. Compliance function

1. An institution shall establish a Compliance function to manage its compliance risk.

2. An institution shall, through its Board of Directors, 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 Board of Directors 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 Board of Directors and the RCF within the decision-making process.

5. The Compliance function should advise the Board of Directors 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.

28. 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 Board of Directors shall ascertain that there is no departure from the internal auditors' requirement 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 Board of Directors.

> 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 Board of Directors 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

29. 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.

30. 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 Banking Rule BR/04 Appendix 4 Section I.4 paragraph 1.1.3 which requires such an independent function for AMA institutions; the tasks of this function are described in the EBA 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

31. 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 Board of Directors and Senior Management 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.

32. 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 Board of Directors in governing the institution.

According to Banking Rule BR/07 paragraph 23, 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 Board of Directors and Senior Management, including attendances to Board and committees' meetings, 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 Board of Directors and Senior Management) 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 Board of Directors 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.