AFME Response to CEBS consultation on the Guidebook on Internal Governance

AFME welcomes the proposed Guidebook on Internal Governance which incorporates CEBS High Level Principles on Remuneration and its High Level Principles on Risk Management in accordance with Article 22 of Directive 2006/48/EC.

We do have specific comments with respect to the principles and supporting paragraphs, which are set out below. However, our main concern is the need for further clarification regarding the nature of duties performed by the board in the unitary board paradigm. In our view it is necessary to delineate between the duties of the board and the duties of senior management. We refer to Principles 5 and 6 of the proposed guidelines.

It is true that the most senior executives of a bank are often also members of the bank's board. These would include the CEO and usually the CFO. There could be others. Although the board as a whole oversees the activities of these most senior managers, the actions of these senior managers as such are not the actions of the board. In our view this principle is blurred by the language of Principle 6, which seems to conflate the two or could be interpreted as doing so. It is our view that the management function being referred to in Principle 6 is actually the function performed by senior management when making proposals to the board for the institution's direction and then ensuring the effective implementation of the strategy through the day-to-day running of the organisation. The board as a whole is not responsible for the day-to-day running of the institution. This lies with the senior executive function. However, the board does oversee the senior management of the company, including the CEO and CFO and other senior executive offices. The CEO as a senior executive will propose to the whole board the direction and strategy for the enterprise, and the board will approve it or not along with risk appetite/tolerance parameters proposed by the CFO/CEO with the advice of the Risk Committee and CRO.

To illustrate our point, we would argue that the responsibility for any failure to remain within the risk parameters set by the board would lie with senior executive management and not with the board as a whole. The board in its supervisory or oversight function will be responsible for monitoring and, if necessary, determining responsibility for any failure by senior executive management. In such a case it should be considered a senior management failure, unless the board has failed to heed information received through the enterprise's control functions or from external sources, or has failed to assure itself that appropriate control functions are in place.

We have another overarching concern. Many of the principles are drafted in a way that could be construed as requiring rigid application of principles on a legal entity basis. Whilst we may broadly agree with many of these principles at a group level, we would not agree with replication of each and all of these concepts if applied on an individual legal entity basis. We would not agree

that the same governance standards applied to the parent should be applied to every subsidiary, unless each entity acts on a standalone basis with regards to areas such as strategy, remuneration, risk framework, etc. Such a model would carry its own risks, and generally global firms employ a central governance overlay to appropriate entity-level controls and governance. We would prefer that the wording be made clearer in this regard but recognise that much will have to be left to the judgement of the relevant board and its Supervisor. The following comments should be read with this position in mind.

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.

We support Principle 1 and have no further comment.

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).

As mentioned in our introductory remarks, we would not agree that the "same internal governance values and policies" (Para. 28) must apply at all levels.

We would not agree with the position that there must be NEDs on each and every subsidiary board (Para. 33). We would qualify the language by adding the following:

"where such is deemed necessary and proportionate given the nature of the subsidiary and the complexity of its activities, given the control functions established by the parent board".

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.

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.

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.

The Principle is fine. With respect to the guidance in Para 42, we would suggest "similar" measures rather than "same" measures be taken when an institution performs certain activities for clients. In Para 41, we would suggest that in the second bullet point information should be "available" to the board and supervisors "in accordance with applicable law". The information need not be "reported" unless it is needed or there has been some breach of policy as set by the board.

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.

We wholly endorse Principle 5. However, guidance in Para 45 should indicate that senior management has the primary responsibility for appropriate communication with supervisory authorities.

It is not sufficiently clear whether these responsibilities are applicable solely at the group level. Whilst many may be applicable to each regulated subsidiary, the language should recognise the influence of the parent in setting policies, etc.

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.

We find Principle 6 confusing unless read in the context of a dual board structure. See our introductory remarks regarding the distinction between functions of the executive management and the board's supervisory function.

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.

Para. 54 & 55 should be clarified:

(i) The Board should include a mix of skills/competencies to allow the Board to function competently as a whole i.e. not all attributes should be required of each individual Board member. Board diversity as advocated by the UK Corporate Governance Code requires that a Board includes a broad range of skill sets which will allow a broad range of views to be expressed to counter group-think

(ii) It does not make sense to us that board members serve a defined term at the subsidiary level (where they are most likely to be serving "at will"). We do not consider long service of the members of the management body to be a problem per se.

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.

Para 57 reads as if all Board members are NEDs, which cannot be the case. We note that with non-listed subsidiary directors it is usual for all, or a high percentage, to be executives because of their role within the firm, and it is also common for such executives to serve on multiple group boards.

We are concerned regarding the first bullet point in Para 60. Disclosed conflicts of interest that can be managed (e.g. an arms-length transaction) may be acceptable to a board. To say that all conflicts of interest should be "avoided" to the extent possible is to practically say that such transactions should not be done. We suggest that the language state that a member's duty is to avoid conflicts of interest that have not been disclosed to and approved by the board but otherwise to ensure that conflicts are managed appropriately.

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.

We believe the reference to "sufficient qualifications" in Para. 64 should be amended to read "skills, knowledge and understanding". In addition, Para. 64 should be a collective test, as an individual test will inhibit the appointment of people with diverse backgrounds.

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 (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.

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.

We suggest the guidance in Para. 71 be amended to indicate that the Chairman and the CEO should not be the same person "unless the board determines that it would be in the best interests of the enterprise".

Para. 72 should also refer to the need to take into account "any group controls applicable to the relevant subsidiary (if it is not a parent entity)".

In Para. 73 we do not agree that there is a need for "a sufficient number of independent members" for committees established at unlisted subsidiaries (assuming "independent implies NEDs). We propose that the requirement that committees, mandates and composition of boards need be limited to listed companies.

Regarding Para. 76, we suggest that the guidance be qualified with the clause "unless the board determines that the most suitable candidate, given the enterprise's circumstances, requires an experienced person even at the cost of some quantum of formal independence." In our view, the board should have the flexibility and the final responsibility to make such determinations.

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.

We propose that the word "operational" in line 3 of Para. 80 should be deleted and the word "reputational" substituted therefore.

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.

We are concerned that the Principle as stated could be interpreted in a way that would disallow transactions or arrangements which may create manageable conflicts. The current language should be amended to say that the conflicts policies should identify actual and potential conflicts of interest so that they can be prevented "or managed". Only unmanageable conflicts need be prevented.

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.

We support Principle 13 and have no further comment.

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.

In our view, the outsourcing policies of the enterprise should be the responsibility of senior management (including through the workings of appropriate committees or control functions) as opposed to the board. Outsourcing is typically not a concern of a bank's board and is more appropriately placed with the senior executives or their delegate who is running the day-to-day operations of the enterprise.

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 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).

Please see our general over-arching comment. We propose that the language take account of the influence of group-wide policies, which may be set and applied at a high level through a central remuneration committee.

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.

We suggest that the guidance in Para. 100 should make clear that there is no need for external review. The risk management framework will be subject to the oversight of the risk committee (taking account of the factors listed) and can also be reviewed independently by Internal Audit.

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) 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.

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 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.

We believe many groups will have substantial subsidiaries and these will need to consider both their own risk and benefits from the work of the firm-wide committee/framework.

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.

Please see our overarching comments regarding this principle. With respect to international financial groups, it should be recognised in the guidance that there will be policies applicable throughout a group. Some groups may have one committee for all entities. Other groups may establish regional committees or even have committees for specific (material) entities.

Principle 24 - Chief Risk Officer

An institution should appoint a person (the 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.

Please see our general over-arching comments regarding international financial groups and the need to take into account firm-wide policies and structures in considering the role of a CRO, while also ensuring the CRO's independence and effectiveness.

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.

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.

The guidance in Para. 160 should make clear that the internal audit function may provide independent monitoring of information systems with or without externally sourced assistance.

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.

We note the importance of the qualifications of Principle 29 stated in Paras. 166 and 167. As a practical matter, companies will provide training and guidance sufficient to enable each staff member to perform his/her responsibilities professionally. There is no need to inform all staff members regarding high level strategies or detailed business strategies that may be confidential and of proprietary value. What is meant by strategies here?

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.

Principle 30 should include a reference to the need to consider competitive and legal concerns. The following language would be helpful if added at the end: "taking into account appropriate competitive and legal considerations of the institution".

We are also concerned with the second bullet point of guidance in Para. 170 which would expose sensitive proprietary information to the public (as opposed to supervisors). In our view, there should not be a requirement to publicly disclose such information. We would suggest that no public disclosure be required in the absence of a legal requirement to do so.

We strongly oppose a requirement of public disclosure of most of the information referenced by the bullet points in the case of unlisted subsidiaries. We also question the need to include material financial information on this list in relation to unlisted subsidiaries, particularly as publicly held corporations already have legal obligations to make financial disclosures.

Conclusion

We thank you for your consideration of this response to your consultation on the draft Guidebook. If it would be helpful to the consultation process, we would be happy to discuss any aspect of the response with the CEBS team at its convenience.

Very truly yours,

William J. Ferrari
Managing Director

About AFME

AFME (Association for Financial Markets in Europe) promotes fair, orderly, and efficient European wholesale capital markets and provides leadership in advancing the interests of all market participants. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants.

AFME participates in a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association through the GFMA (Global Financial Markets Association).

AFME is listed on the EU Register of Interest Representatives, registration number 65110063986-76.

For more information please visit the AFME website, www.afme.eu.