Principles for enhancing corporate governance issued by Basel Committee

Comments of IFACI's Banking Professional Group

Principle 3
The board should define appropriate governance practices for its own work and have in place the means to ensure such practices are followed and periodically reviewed for improvement.

Board Committees
48. For large banks and internationally active banks, an audit committee or equivalent should be required. The audit committee typically is responsible for the financial reporting process; providing oversight of the bank's internal and external auditors; approving, or recommending to the board or shareholders for their approval, the appointment, compensation and dismissal of external auditors; reviewing and approving the audit scope and frequency; receiving audit reports; and ensuring that senior management (with the appropriate involvement from the control functions) is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations and other problems identified by auditors. In addition, the audit committee should oversee the establishment of accounting policies by the bank.

IFACI's Comments: We would appreciate to see clearly Internal Audit mentioned "for their approval the appointment and dismissal of the head of Internal audit" to increase its independence.

---

50. It is also appropriate for many banks, especially large banks and internationally active banks, to have a board-level risk committee or equivalent, responsible for advising the board on the bank's overall current and future risk tolerance/appetite and strategy, and for overseeing senior management's implementation of that strategy. This should include strategies for capital and liquidity management, as well as for credit, market, operational, compliance, reputational and other risks of the bank. To enhance the effectiveness of the risk committee, it should receive formal and informal communication from the bank's risk management function and chief risk officer (see Principle 6), and should, where appropriate, have access to external expert advice, particularly in relation to proposed strategic transactions, such as mergers and acquisitions.

IFACI's Comments: We would appreciate to see Internal Audit as an external expert vis-à-vis the Board.

Principle 5
Under the direction of the board, senior management should ensure that the bank's activities are consistent with the business strategy, risk tolerance/appetite and policies approved by the board.

66. Senior management should implement appropriate systems for managing the risks - both financial and non-financial - to which the bank is exposed. This includes a comprehensive and independent risk management function and an effective system of internal controls. These should be

designed and operated to ensure adherence to the bank's strategy and risk tolerance/appetite (which should also be in line with each other, as discussed in greater detail in Principles 6-7 below).

IFACI's Comments: We would appreciate to see clearly mentioned with a strong internal audit function.

Principle 6
Banks should have an independent risk management function (including a chief risk officer or equivalent) with sufficient authority, stature, independence, resources and access to the board.
Risk management vs. internal controls

67. Risk management generally encompasses the process of:

- *identifying key risks to the bank;*
- *measuring exposures to those risks;*
- *monitoring risk exposures and determining the corresponding capital needs (ie capital planning) on an ongoing basis;*
- *taking steps to control or mitigate risk exposures; and*
- *reporting to senior management and the board on all the items noted in this paragraph.*

IFACI's comments: It is important to confirm that the Internal Audit is not part of Risk Management. We recommend to clearly state that Internal Audit is totally separated from Risk Management

---

Chief risk officer or equivalent
69. Large banks and internationally active banks, and others depending on their risk profile and local governance requirements, should have an independent senior executive with distinct responsibility for the risk management function and the institution's comprehensive risk management framework across the entire organisation. This executive is commonly referred to as the chief risk officer (CRO). Since some banks may have an officer who fulfils the function of a CRO but has a different title, reference in this guidance to the CRO is intended to incorporate equivalent positions. Whatever the title, at least in large banks, the role of the CRO should be distinct from other executive functions and business line responsibilities, and there generally should be no "dual hatting" (ie the chief operating officer, CFO or other senior management should not also serve as the CRO).25

70. Formal reporting lines may vary across banks, but regardless of these reporting lines, the independence of the CRO is paramount. While the CRO may report to the CEO or other senior management, the CRO should also report and have direct access to the board and its risk committee without impediment. Interaction between the CRO and the board should occur regularly and be documented adequately. Non-executive board members should have the right to meet regularly - in the absence of senior management - with the CRO.

71. The CRO should have sufficient stature, authority and seniority within the organisation. This will typically be reflected in the ability of the CRO to influence decisions that affect the bank's exposure to risk. Beyond periodic reporting, the CRO should thus have the ability to engage with the board and other senior management on key risk issues and to access such information as the CRO deems necessary to form his or her judgement. Such interactions should not compromise the CRO's independence.

72. If the CRO is removed from his or her position for any reason, this should be done with the prior approval of the board and generally should be disclosed publicly. The bank should also discuss the reasons for such removal with its supervisor.

Scope of responsibilities, stature and independence of the risk management function

73. The risk management function is responsible for identifying, measuring, monitoring, controlling or mitigating, and reporting on risk exposures. This should encompass all risks to the bank, on- and off-balance sheet and at a group-wide, portfolio and business-line level.

74. The risk management function, under the direction of the CRO, should have sufficient stature within the bank such that issues raised by risk managers receive the necessary attention from the board, senior management and business lines. Business decisions by the bank typically are a product of many considerations. By properly positioning and supporting its risk management function, a bank helps ensure that the views of risk managers will be an important part of those considerations.

75. While it is not uncommon for risk managers to work closely with individual business units and, in some cases, to have dual reporting lines, the risk management function should be sufficiently independent of the business units whose activities and exposures it reviews. While such independence is an essential component of an effective risk management function, it is also important that risk managers are not so isolated from business lines - geographically or otherwise - that they cannot understand the business or access necessary information. Moreover, the risk management function should have access to all business lines that have the potential to generate material risk to the bank. Regardless of any responsibilities that the risk management function may have to business lines and senior management, its ultimate responsibility should be to the board.

Resources

76. A bank should ensure through its planning and budgeting processes that the risk management function has adequate resources (in both number and quality) necessary to assess risk, including personnel, access to information technology systems and systems development resources, and support and access to internal information. These processes should also explicitly address and provide sufficient resources for internal audit and compliance functions. Compensation and other incentives (eg opportunities for promotion) of the CRO and risk management staff should be sufficient to attract and retain qualified personnel.

Qualifications

77. Risk management personnel should possess sufficient experience and qualifications, including market and product knowledge as well as mastery of risk disciplines.26 Staff should have the ability and willingness to challenge business lines regarding all aspects of risk arising from the bank's activities.

IFACI's comments: The principal roles of Risk Management are defined in article 67. We think however that it would be useful to give a more precise definition of what Risk Management (defined under French Regulations as "Filière Risque") actually is and what this function ("filière") actually covers. Also we ask the question whether the "filière risque" has to encompass all the key risks, because some risks are of very different nature and managed by very different people in the organization. In this respect, it may be in some cases rather unrealistic to have one CRO in charge of all the risks.

72. If the CRO is removed from his or her position for any reason, this should be done with the prior approval of the board and generally should be disclosed publicly. The bank should also discuss the reasons for such removal with its supervisor.

IFACI's comments: We would appreciate to have the same principle for internal audit. The same principle should be added for audit in principle 9 (see below). This point is important for independence of the audit in case this point is maintained for CRO.

---

75. […] Regardless of any responsibilities that the risk management function may have to business lines and senior management, its ultimate responsibility should be to the board.

IFACI's comments: We would like to see the same comment for Internal Audit considering that audit could be considered not being the last level of control

---

Resources

76. A bank should ensure through its planning and budgeting processes that the risk management function has adequate resources (in both number and quality) necessary to assess risk, including personnel, access to information technology systems and systems development resources, and support and access to internal information. These processes should also explicitly address and provide sufficient resources for internal audit and compliance functions. Compensation and other incentives (eg opportunities for promotion) of the CRO and risk management staff should be sufficient to attract and retain qualified personnel.

IFACI's comments: We would like to see the last sentence applying as well to audit. We suggest to add "and audit staff in order for audit to maintain its credibility".

Principle 9

The board and senior management should effectively utilize the work conducted by internal audit functions, external auditors and internal control functions.

96. The board should recognize and acknowledge that independent, competent and qualified internal and external auditors, as well as other internal control functions (including the compliance functions), are vital to the corporate governance process in order to achieve a number of important objectives. Senior management should also recognize the importance of the effectiveness of these functions to the long-term soundness of the bank.

IFACI's comments: Please see Principle 6 - § 72

---

97. The board and senior management can enhance the ability of the internal audit function to identify problems with a bank's risk management and internal control systems by:

- *encouraging internal auditors to adhere to national and international professional standards, such as those established by the Institute of Internal Auditors;*
- *promoting the independence of the internal auditor, for example by ensuring that internal audit reports and/or has direct access to the board or the board's audit committee;*

- *recognising the importance of the audit and internal control processes and communicating their importance throughout the bank;*
- *utilising, in a timely and effective manner, the findings of internal audits and requiring timely correction of identified problems by senior management; and*
- *engaging internal auditors to judge the effectiveness of the risk management and compliance function, including the quality of risk reporting to the board and senior management, as well as the effectiveness of other key control functions.*

IFACI's comments: As it is explained in article 97, Internal Audit has to judge the effectiveness of the risk management ("filière risque"). In our opinion, it should also be clearly stated that Internal Audit is the ultimate level of assessment of the "Filière risque".

Principle 10

The board should actively oversee the compensation system's design and operation, and should monitor and review the compensation system to ensure that it operates as intended.

106. The compensation of the control function (eg CRO and risk management staff) should be structured in a way that is based principally on the achievement of their objectives and does not compromise their independence (eg compensation should not be substantially tied to business line revenue).

IFACI's comments: We would appreciate to have internal audit included in the same compensation principle.

The role of supervisors

2. Supervisors should regularly perform a comprehensive evaluation of a bank's overall corporate governance policies and practices and evaluate the bank's implementation of the principles.

135. Supervisors should evaluate whether the bank has in place effective mechanisms through which the board and senior management execute their oversight responsibilities. In addition to policies and processes, such mechanisms include properly positioned and staffed control functions, such as internal audit, risk management and compliance. In this regard, supervisors should assess the effectiveness of oversight of these functions by the bank's board. This could include assessing the extent to which the board interacts with and meets with the representatives of the control functions. Supervisors should ensure that the internal audit function conducts independent, risk-based and effective audits. This includes conducting periodic reviews of the bank's control functions and of the overall internal controls. Supervisors should assess the adequacy of internal controls that foster sound governance and how well they are being implemented.

IFACI's comments: We noticed that this consultative document mainly refers to 3 elements of internal control: risk management ("filière risque"), compliance and internal audit, but not to permanent control as such. In this respect, this document differs from French Regulations which includes permanent control as an important element of internal control. That may create a difficulty for French Institutions. As far as the permanent control as a function is relevant here, the relations and interactions of permanent control between Risk Management ("filière risque"), compliance and Internal Audit should also be addressed in this document.

---

3. Supervisors should supplement their regular evaluation of a bank's corporate governance policies and practices by monitoring a combination of internal reports and prudential reports.

138. For monitoring and evaluation purposes, the supervisor should periodically review key internal reports of the bank. To make meaningful comparisons between banks, the supervisor may also require a standardized supervisory reporting process, covering the data items the supervisor deems necessary.

IFACI's comments: Audit reports are concerned as well as risk management report, etc. Supervisor is already asking some of them and audit committee reports, etc.