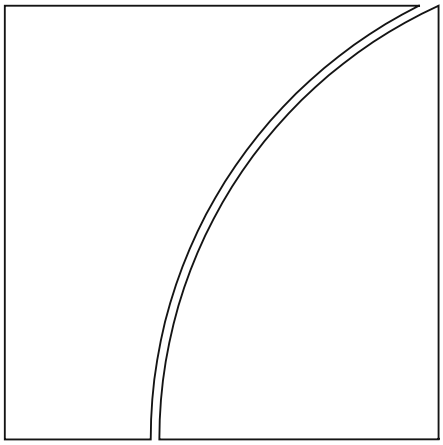
Basel Committee on Banking Supervision

Consultative document

Guidelines



Corporate governance principles for banks

Issued for comments by 9 January 2015

October 2014

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9131-927-5 (print)
ISBN 978-92-9131-905-3 (online)

Contents

Glossary

Bank or banking organisation: Banks, bank holding companies or other companies considered by banking supervisors to be the parent of a banking group under applicable national law as determined to be appropriate by the entity's national supervisor.

Board of directors or board: The group structure that supervises management. The structure of the board differs among countries.[1] The use of "board" throughout this paper encompasses the different national models that exist and should be interpreted in accordance with applicable law within each jurisdiction.

Corporate governance: A set of relationships between a company's management, its board, its shareholders and other stakeholders which provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance.[2] It helps define the way authority is allocated and how corporate decisions are made.

Control functions: Those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function.

Duty of care: The duty of board members to decide and act on an informed and prudent basis with respect to the bank. Often interpreted as requiring board members to approach the affairs of the company the same way that a "prudent person" would approach his or her own affairs.[2]

Duty of loyalty: The duty of board members to act in good faith in the interest of the company. The duty of loyalty should prevent individual board members from acting in their own interest, or the interest of another individual or group, at the expense of the company and shareholders.[2]

Executive director: In jurisdictions where this is permitted, a member of the board (eg director) who also has management responsibilities within the bank.[3]

Independent director: For the purposes of this paper, a member of the board who does not have any management responsibilities with the bank and is not under any other undue influence, internal or external, that would impede the board member's exercise of objective judgment.[3]

Internal control system: A set of rules and controls governing the bank's organisational and operational structure including reporting processes, and functions for risk management, compliance and internal audit.

Non-executive director: A member of the board who does not have management responsibilities within the bank.[3]

Risk appetite: The aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.[4]

Risk appetite framework (RAF): The overall approach, including policies, processes, controls and systems though which risk appetite is established, communicated and monitored. It includes a risk

[1] See paragraph 15.

[2] See the glossary of corporate governance-related terms in Organisation for Economic Co-operation and Development (OECD), *Experiences from the Regional Corporate Governance Roundtables,* 2003.

[3] See Financial Stability Board (FSB), *Thematic review on risk governance*, February 2013.

	appetite statement, risk limits and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the RAF. The RAF should consider material risks to the bank, as well as to its reputation vis-à-vis policyholders, depositors, investors and customers. The RAF aligns with the bank's strategy.[4]
Risk appetite statement (RAS):	The written articulation of the aggregate level and types of risk that a bank will accept, or avoid, in order to achieve its business objectives. It includes quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate. It should also include qualitative statements to address reputation and conduct risks as well as money laundering and unethical practices.[4]
Risk capacity:	The maximum amount of risk a bank is able to assume given its capital base, risk management and control measures, as well as its regulatory constraints.
Risk culture:	A bank's norms, attitudes and behaviours related to risk awareness, risk taking and risk management and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume.[5]
Risk governance framework:	As part of the overall corporate governance framework, the framework through which the board and management establish and make decisions about the bank's strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits vis-à-vis the bank's strategy; and identify, measure, manage and control risks.[3]
Risk limits:	Specific quantitative measures or limits based on, for example, forward-looking assumptions that allocate the bank's aggregate RAS to business lines, legal entities as relevant, specific risk categories, concentrations and, as appropriate, other measures.[4]
Risk management:	The processes established to ensure that all material risks and associated risk concentrations are identified, measured, limited, controlled, mitigated and reported on a timely and comprehensive basis.
Risk profile:	Point in time assessment of the bank's gross (ie before the application of any mitigants) or, as appropriate, net risk exposures (ie after taking into account mitigants) aggregated within and across each relevant risk category based on current or forward-looking assumptions.[4]

[4] See FSB, *Principles for an effective risk appetite framework,* November 2013.

[5] See FSB, *Guidance on supervisory interaction with financial institutions on risk culture,* April 2014.

Corporate governance principles for banks

Introduction

1. Effective corporate governance is critical to the proper functioning of the banking sector and the economy as a whole. Banks serve a crucial role in the economy by intermediating funds from savers and depositors to activities that support enterprise and help drive economic growth. Banks' safety and soundness are key to financial stability, and the manner in which they conduct their business, therefore, is central to economic health. Governance weaknesses at banks that play a significant role in the financial system can result in the transmission of problems across the banking sector and the economy as a whole.

2. Corporate governance determines the allocation of authority and responsibilities by which the business and affairs of a bank are carried out by its board and senior management, including how they:

- set the bank's strategy and objectives;
- select and oversee personnel;
- operate the bank's business on a day-to-day basis;
- protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders;
- align corporate culture, corporate activities and behaviour with the expectation that the bank will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations; and
- establish control functions.

3. Supervisors have a keen interest in sound corporate governance as it is an essential element in the safe and sound functioning of a bank and may adversely affect the bank's risk profile if not operating effectively. Well governed banks contribute to the maintenance of an efficient and cost-effective supervisory process, as there is less need for supervisory intervention.

4. Sound corporate governance may permit the supervisor to place more reliance on the bank's internal processes. In this regard, supervisory experience underscores the importance of having the appropriate levels of authority, responsibility, accountability, and checks and balances within each bank, including those of senior management but also of the board of directors and the risk, compliance and internal audit functions.

5. The Basel Committee's October 2010 *Principles for enhancing corporate governance* represented a consistent development in the Committee's longstanding efforts to promote sound corporate governance practices for banking organisations. The 2010 principles sought to reflect key lessons from the 2008–09 financial crisis, and enhance how banks govern themselves and how supervisors oversee this critical area.

6. Since 2010, the Committee and its member jurisdictions have witnessed banks strengthening their overall governance practices and supervisors enhancing their oversight processes.

- In general, banks exhibit a better understanding of the important elements of corporate governance such as effective board oversight, rigorous risk management, strong internal controls, compliance and other related areas. In addition, many banks have made progress in assessing collective board skills and qualifications, instituting standalone board risk committees,

establishing and elevating the role of Chief Risk Officer (CRO), and integrating discussions between board audit and risk committees.

- National authorities have taken measures to improve regulatory and supervisory oversight of corporate and risk governance at banks. These measures include developing or strengthening existing regulation or guidance, raising supervisory expectations for the risk management function, engaging more frequently with the board and management, and assessing the accuracy and usefulness of the information provided to the board.

7. In order to assess the progress of national authorities and the banking industry in the area of risk governance since the global financial crisis, the Financial Stability Board (FSB) issued a *Thematic review on risk governance* in February 2013 as part of its series of peer reviews. The peer review found that financial institutions and national authorities have taken measures to improve risk governance. However, more work is needed by both national authorities and banks to establish effective risk governance frameworks and to enumerate expectations for third-party reviews of the framework. Banks also need to enhance the authority and independence of CROs. National authorities need to strengthen their ability to assess the effectiveness of a bank's risk governance and its risk culture and should engage more frequently with the board and its risk and audit committees.

8. In the light of ongoing developments in corporate governance, and to take account of the FSB peer review recommendations and other recent papers addressing corporate governance issues, the Committee has decided to revisit the 2010 guidance.[6]

9. One of the primary objectives of this revision is to explicitly reinforce the collective oversight and risk governance responsibilities of the board. Another important objective is to emphasise key components of risk governance such as risk culture, risk appetite and their relationship to a bank's risk capacity. The revised guidance also delineates the specific roles of the board, board risk committees, senior management and the control functions including the CRO and internal audit. Another key emphasis is strengthening banks' overall checks and balances.

10. Importantly, the FSB underscored the critical role of the board and the board risk committees in strengthening a bank's risk governance. This includes greater involvement in evaluating and promoting a strong risk culture in the organisation; establishing the organisation's risk appetite and conveying it through the risk appetite statement (RAS); and overseeing management's implementation of the risk appetite and overall governance framework.

11. The increased focus on risk and the supporting governance framework includes identifying the responsibilities of different parts of the organisation for addressing and managing risk. Often referred to as the "three lines of defence", each of the three lines has an important role to play. The business line – the first line of defence – has "ownership" of risk whereby it acknowledges and manages the risk that it incurs in conducting its activities. The risk management function is responsible for further identifying, measuring, monitoring and reporting risk on an enterprise-wide basis as part of the second line of defence, independently from the first line of defence. The compliance function is also deemed part of the second line of defence. The internal audit function is charged with the third line of defence, conducting risk-based and general audits and reviews to provide assurance to the board that the overall

[6] The FSB recommended that member jurisdictions strengthen their regulatory and supervisory guidance for financial institutions, in particular for systemically important financial institutions (SIFIs), on sound risk governance practices. In addition, the FSB recently issued additional guidance on risk appetite frameworks and supervisory assessments of risk culture. Work by the Joint Forum and others since 2010 has also increased the focus on the challenges of supervising groups and conglomerates. This, in turn, has raised important questions about group governance, including expectations for parent company and subsidiary governance and how supervisors can best supervise these institutions.

governance framework, including the risk governance framework, is effective and that policies and processes are in place and consistently applied.

Jurisdictional differences

12. This document is intended to guide the actions of board members, senior managers, control function heads and supervisors of a diverse range of banks in a number of countries with varying legal and regulatory systems, including both Committee member and non-member jurisdictions. The Committee recognises that there are significant differences in the legislative and regulatory frameworks across countries, which may restrict the application of certain principles or provisions therein. Each jurisdiction should apply the provisions as the national authorities see fit. In some cases, this may involve legal change. In other cases, a principle may require slight modification in order to be implemented.

Applicability, proportionality and differences in governance approaches

13. The implementation of these principles should be commensurate with the size, complexity, structure, economic significance and risk profile of the bank and the group (if any) to which it belongs. This means making reasonable adjustments where appropriate for banks with lower risk profiles, and being alert to the higher risks that may accompany more complex and publicly listed institutions.[7] Systemically important financial institutions (SIFIs) are expected to have in place the corporate governance structure and practices commensurate with their role in and potential impact on national and global financial stability.

14. The principles set forth in this document are applicable regardless of whether or not a jurisdiction chooses to adopt the Committee's regulatory framework. The board and senior management at each bank have an obligation to pursue good governance.

15. This document refers to a governance structure composed of a board of directors and senior management. The latter is sometimes called the executive committee, the executive board or the management board. Some countries use a formal two-tier structure, where the supervisory function of the board is performed by a separate entity known as a supervisory board or audit and supervisory board, which has no executive functions. Other countries use a one-tier structure in which the board of directors has a broader role. Still other countries have moved or are moving to a mixed approach that discourages or prohibits executives from serving on the board of directors or limits their number and/or requires the board and board committees to be chaired only by non-executive or independent board members. Some countries also prohibit the CEO from serving as chair of the board of directors or even from being part of the board of directors.

16. Owing to these differences, this document does not advocate any specific board or governance structure. The term board of directors is used as a way to refer to the oversight function and the term senior management as a way to refer to the management function in general. These terms should be interpreted throughout the document in accordance with the applicable law within each jurisdiction.

[7] The Committee recognises that some countries have governance, accounting and auditing standards which may be more extensive and prescriptive for larger or for publicly-listed institutions than the principles set forth in this document.

Recognising that different structural approaches to corporate governance exist across countries and that these structures evolve over time, this document encourages legislators, supervisors, banks and others to frequently review their practices so as to strengthen checks and balances and sound corporate governance under diverse structures. The application of corporate governance standards in any jurisdiction is naturally expected to be pursued in a manner consistent with applicable national laws, regulations and codes (eg taking into consideration the existence of oversight boards in some jurisdictions).

17. One fundamental corporate governance issue in respect of publicly listed companies is shareholder rights. Such rights are not the primary focus of this guidance and are addressed in the corporate governance principles issued by the OECD.[8] However, the Committee recognises the importance of shareholder rights and of responsible shareholder engagement. The Committee also recognises the importance of exercise of shareholder rights, particularly when certain shareholders have the right to have a representative on the board. In such cases, the suitability of the appointed board member is as critical as their awareness of the responsibility to look after the interests of the bank as a whole, not just of the shareholders.

18. Effective implementation of sound corporate governance requires relevant legal, regulatory and institutional foundations. A variety of factors, including the system of business laws, stock exchange rules and accounting standards, can affect market integrity and systemic stability. Such factors, however, are often outside the scope of banking supervision. Supervisors are nevertheless encouraged to be aware of legal and institutional impediments to sound corporate governance, and to take steps to foster effective foundations for corporate governance where it is within their legal authority to do so. Where it is not, supervisors may wish to consider supporting legislative or other reforms that would allow them to have a more direct role in promoting or requiring sound corporate governance.

19. The principles of sound corporate governance should also be applied to state-owned or state-supported banks, including when such support is temporary.[9]

[8] See OECD, *Principles of corporate governance*, 2004, www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf. In 2014, the OECD launched a review of the principles to ensure their continuing high quality, relevance and usefulness, taking into account recent developments in the corporate sector and capital markets.

[9] See also OECD, *Guidelines on corporate governance of state-owned enterprises*, www.oecd.org/daf/ca/oecdguidelinesoncorporategovernanceofstate-ownedenterprises.htm.

Principle 1: Board's overall responsibilities

The board has overall responsibility for the bank, including approving and overseeing the implementation of the bank's strategic objectives, governance framework and corporate culture. The board is also responsible for providing oversight of senior management.

Responsibilities of the board

20. The board has ultimate responsibility for the bank's business strategy and financial soundness, key personnel decisions, internal organisation and governance structure and practices, and risk management and compliance obligations.

21. The board should ensure[10] that the bank's organisational structure enables the board and senior management to carry out their responsibilities and facilitates effective decision-making and good governance. This includes clearly laying out the key responsibilities and authorities of the board itself, of senior management and of those responsible for the control functions.

22. The members of the board should exercise their "duty of care" and "duty of loyalty" to the bank under applicable national laws and supervisory standards. This includes actively engaging in the major matters of the bank and keeping up with material changes in the bank's business and the external environment as well as acting in a timely manner to protect the long-term interests of the bank.

23. Accordingly, the board should:

- establish and monitor the bank's business objectives and strategy;
- establish the bank's corporate culture and values;
- oversee implementation of the appropriate governance framework;
- develop, along with senior management and the CRO, the bank's risk appetite, taking into account the competitive and regulatory landscape, long-term interests, exposure to risk and the ability to manage risk effectively;
- monitor the bank's adherence to the RAS, risk policy and risk limits;
- approve and oversee the implementation of the bank's capital adequacy assessment process, capital and liquidity plans, compliance policies and obligations, and the internal control system;
- approve the selection and oversee the performance of senior management; and
- oversee the design and operation of the bank's compensation system, and monitor and review the system to ensure that it is aligned with the bank's desired risk culture and risk appetite.

24. The board should ensure that transactions with related parties (including internal group transactions) are reviewed to assess risk and are subject to appropriate restrictions (eg by requiring that such transactions be conducted on arm's length terms) and that corporate or business resources of the bank are not misappropriated or misapplied.

[10] Throughout this document, the phrase "the board should ensure" is used to convey the Committee's view that a board of directors has ultimate responsibility for the bank's adoption of the necessary processes, policies, procedures, controls and hiring of sufficient staff to achieve the function or objective described.

25. The board should review the governance framework periodically so that it remains appropriate in the light of material changes in the bank's size, complexity, geographic reach, business strategy, market and governance best practices, and regulatory requirements.

26. In discharging these responsibilities, the board should take into account the legitimate interests of depositors, shareholders and other relevant stakeholders. It should also ensure that the bank maintains an effective relationship with its supervisors.

Corporate culture and values

27. A fundamental component of good governance is a demonstrated corporate culture of reinforcing appropriate norms for responsible and ethical behaviour. These norms are especially critical in terms of a bank's risk awareness, risk-taking and risk management.

28. In order to promote a sound corporate culture, the board should take the lead in establishing the "tone at the top" by:

- setting and adhering to corporate values for itself, senior management and other employees that create expectations that all business should be conducted in a legal and ethical manner;
- promoting risk awareness within a strong risk culture, conveying the board's expectation that it does not support excessive risk-taking and that all employees are responsible for helping ensure that the bank operates within the agreed risk appetite and risk limits;
- ensuring that appropriate steps are taken to communicate throughout the bank the corporate values, professional standards or codes of conduct it sets, together with supporting policies; and
- ensuring that employees, including senior management, are aware that appropriate disciplinary or other actions will follow unacceptable behaviours and transgressions.

29. A bank's code of conduct or code of ethics, or comparable policy, should define acceptable and unacceptable behaviours.

- It should explicitly disallow behaviour that could lead to any reputation risks or improper or illegal activity, such as financial misreporting, money laundering, fraud, anti-competitive practices, bribery and corruption, or the violation of consumer rights.
- It should make clear that employees are expected to conduct themselves ethically in addition to complying with laws, regulations and company policies.

30. The bank's corporate values should recognise the critical importance of timely and frank discussion and escalation of problems to higher levels within the organisation.

- Employees should be encouraged and able to communicate, confidentially and without the risk of reprisal, legitimate concerns about illegal, unethical or questionable practices. This can be facilitated through a well communicated policy and adequate procedures and processes, consistent with national law, which allow employees to communicate material and bona fide concerns and observations of any violations in a confidential way (eg whistle blower policy). This includes communicating material concerns to the bank's supervisor.
- There should be direct or indirect communications to the board (eg through an independent audit or compliance process or through an ombudsman independent of the internal "chain of command").
- The board should determine how and by whom legitimate concerns shall be investigated and addressed by an objective independent internal or external body, senior management and/or the board itself.

Risk appetite, management and control

31. As part of the overall corporate governance framework, the board is responsible for overseeing a strong risk governance framework. An effective risk governance framework includes a strong risk culture, a well developed risk appetite framework articulated through the RAS, and well defined responsibilities for risk management in particular and control functions in general.

32. Developing and conveying the bank's RAS is essential to reinforcing a strong risk culture. The board should clearly outline actions to be taken when stated risk limits are breached, including disciplinary actions for excessive risk-taking, escalation procedures and board of director notification.

33. The board should take an active role in developing the risk appetite and ensuring its alignment with the bank's strategic, capital and financial plans and compensation practices. The bank's risk appetite should be clearly conveyed through an RAS that is easily understood by all relevant parties: the board itself, senior management, bank employees and the supervisor.

34. The bank's RAS should:

- include both quantitative and qualitative considerations;
- establish the individual and aggregate level and types of risk that the bank is willing to assume in advance of and in order to achieve its business activities within its risk capacity;
- define the boundaries and business considerations in accordance with which the bank is expected to operate when pursuing the business strategy; and
- communicate the board's risk appetite effectively throughout the bank, linking it to daily operational decision-making and establishing the means to raise risk issues and strategic concerns across the bank.

35. The development of an effective RAS should be driven by both top-down board leadership and bottom-up management involvement. While risk appetite development may be initiated by senior management, successful implementation depends upon effective interactions between the board, senior management, risk management and operating businesses including the chief financial officer.

36. A risk governance framework should include well defined organisational responsibilities for risk management, typically referred to as the three lines of defence:

- the business line;
- a risk management function and a compliance function independent from the first line of defence; and
- an internal audit function independent from the first and second lines of defence.[11]

37. Depending on the bank's nature, size and complexity, and the risk profile of its activities, the specifics of how these three lines of defence are structured can vary. Regardless of the structure, responsibilities for each line of defence should be well defined and communicated.

38. Business units are the first line of defence. They take risks and are responsible and accountable for the ongoing management of such risks. This includes identifying, assessing and reporting such exposures, taking into account the bank's risk appetite and its policies, procedures and controls. The

[11] See Basel Committee on Banking Supervision (BCBS), *Principles for sound operational risk management*, www.bis.org/publ/bcbs195.pdf and *The internal audit function in banks*, www.bis.org/publ/bcbs223.pdf.

manner in which the business line executes its responsibilities should reflect the bank's existing risk culture.

39. The second line of defence includes an independent and effective risk management function. The risk management function complements the business line's risk activities through its monitoring and reporting responsibilities. Among other things, it is responsible for overseeing the bank's risk-taking activities and assessing risks and issues independently from the business line. The function should promote the importance of senior management and business line managers in identifying and assessing risks critically rather than relying only on surveillance conducted by the risk management function.

40. The second line of defence also includes an independent and effective compliance function. The compliance function should, among other things, routinely monitor compliance with laws, corporate governance rules, regulations, codes and policies to which the bank is subject. The board should approve compliance policies that are communicated to all staff. The compliance function should ensure that the compliance policies are observed and report to senior management and, as appropriate, to the board on how the bank is managing its compliance risk. The function should also have sufficient authority, stature, independence, resources and access to the board.

41. The third line of defence consists of an independent and effective internal audit function. Among other things, it provides independent review and assurance on the quality and effectiveness of the bank's risk governance framework including links to organisational culture, as well as strategic and business planning, compensation and decision-making processes. Internal auditors must be competent and appropriately trained and not involved in developing, implementing or operating the risk management function (see Principle 9).

42. The board should ensure that the risk management, compliance and audit functions are properly positioned, staffed and resourced and carry out their responsibilities independently and effectively. In the board's oversight of the risk governance framework, the board should regularly review policies and controls with senior management and with the heads of the risk management, compliance and audit functions to identify and address significant risks and issues, as well as determine areas that need improvement.

Oversight of senior management

43. The board should select the CEO and may select other key members of senior management, as well as the heads of the control functions.

44. The board should provide oversight of senior management. It should hold members of senior management accountable for their actions and enumerate the consequences if those actions are not aligned with the board's performance expectations. This includes adhering to the bank's values, risk appetite and risk culture, regardless of financial gain or loss to the bank. In doing so, the board should:

- monitor that senior management's actions are consistent with the strategy and policies approved by the board, including the risk appetite;
- meet regularly with senior management;
- question and critically review explanations and information provided by senior management;
- set appropriate performance and remuneration standards for senior management consistent with the long-term strategic objectives and the financial soundness of the bank;
- ensure that senior management's knowledge and expertise remain appropriate given the nature of the business and the bank's risk profile; and
- ensure that appropriate succession plans are in place for senior management positions.

Principle 2: Board qualifications and composition

Board members should be and remain qualified, individually and collectively, for their positions. They should understand their oversight and corporate governance role and be able to exercise sound, objective judgment about the affairs of the bank.

Board composition

45. The board must be suitable to carry out its responsibilities and have a composition that facilitates effective oversight. For that purpose, the board should be comprised of a sufficient number of independent directors.

46. The board should be comprised of individuals with a balance of skills, diversity and expertise, who collectively possess the necessary qualifications commensurate with the size, complexity and risk profile of the bank.

47. In assessing the collective suitability of the board, the following should be taken into account:

- Board members should have a range of knowledge and experience in relevant areas and have varied backgrounds to promote diversity of views. Relevant areas of competence include financial and capital markets, financial analysis, financial stability, strategic planning, risk management, compensation, regulation, corporate governance and management skills.
- The board collectively should have a reasonable understanding of local, regional and, if appropriate, global economic and market forces and of the legal and regulatory environment. International experience, where relevant, should also be considered.
- Where board expertise is insufficient in any of the above areas, the board should be able to employ independent experts as needed.

Board member selection and qualifications

48. Boards should have a clear and rigorous process for identifying, assessing and selecting board candidates. Unless required otherwise by law, the board (not management) identifies and nominates[12] candidates and ensures appropriate succession planning of board members and senior management.

49. The selection process should include reviewing whether board candidates: (i) possess the knowledge, skills, experience and independence of mind given their responsibilities on the board and in the light of the bank's business and risk profile; (ii) have a record of integrity and good repute; and (iii) have sufficient time to fully carry out their responsibilities.

50. Board candidates should not have any conflicts of interest that may impede their ability to perform their duties objectively and subject them to undue influence from:

- other persons (such as management or other shareholders);
- past or present positions held; or

[12] The Committee acknowledges that in some jurisdictions shareholders or other stakeholders have the right to nominate board members and/or to approve their selection. In such cases, the board should still do whatever is within its power to ensure that members selected for the board are qualified.

- personal, professional or other economic relationships with other members of the board or management (or with other entities within the group).

51. If a board member ceases to be qualified or is failing to fulfil his or her responsibilities, the board should take appropriate actions as permitted by law, which may include notifying their banking supervisor.

52. The bank should have in place a nomination committee or similar body, composed of a sufficient number of independent board members, which identifies and nominates candidates after having taken into account the criteria described above.

- The nomination committee should analyse the responsibilities relating to the role the board member will play and the knowledge, experience and competence which the role requires.
- Where a supervisory board or board of auditors is formally separate from a management board, objectivity and independence still need to be assured by appropriate selection of board members.[13]
- The nomination committee should strive to ensure that the board is not dominated by any one individual or small group of individuals in a manner that is detrimental to the interests of the bank as a whole.

53. In order to help board members acquire, maintain and enhance their knowledge and skills, and fulfil their responsibilities, the board should ensure that members participate in induction programmes and have access to ongoing training on relevant issues. The board should dedicate sufficient time, budget and other resources for this purpose, and draw on external expertise as needed. More extensive efforts should be made to train and keep updated those members with more limited financial, regulatory or risk-related experience.

54. Where there are shareholders with power to appoint board members, the board should ensure such board members understand their duties. Board members have responsibilities to the bank's overall interests, regardless of who appoints them. In cases where board members are selected by a controlling shareholder, the board may wish to set out specific procedures or conduct periodic reviews to ensure the appropriate discharge of responsibility by all board members.

[13] If a former executive of the bank is being considered to serve on the board of the bank, the board should carefully review any potential conflicts of interest that might arise, particularly if this person is to carry out the role of chair of the board or of a committee of the board. If the board deems it to be in the interest of the bank to have this person serve on the board, appropriate processes to mitigate the potential conflicts of interest should be put in place, such as a waiting period and/or a description of matters on which the person should recuse himself or herself to avoid a conflict of interest.

Principle 3: Board's own structure and practices

The board should define appropriate governance structures and practices for its own work, and put in place the means for such practices to be followed and periodically reviewed for ongoing effectiveness.

Organisation and assessment of the board

55. The board should structure itself in terms of leadership, size and the use of committees so as to effectively carry out its oversight role and other responsibilities. This includes ensuring that the board has the time and means to cover all necessary subjects in sufficient depth and have a robust discussion of issues.

56. The board should maintain and periodically update organisational rules, by-laws, or other similar documents setting out its organisation, rights, responsibilities and key activities.

57. To support its own performance, the board should carry out regular assessments – alone or with the assistance of external experts – of the board as a whole, its committees and individual board members. The board should:

- periodically review its structure, size and composition;
- assess the ongoing suitability of each board member periodically (at least annually) also taking into account his or her performance on the board;
- either separately or as part of these assessments, periodically review the effectiveness of its own governance practices and procedures, determine where improvements may be needed, and make any necessary changes; and
- use the results of these assessments as part of the ongoing improvement efforts of the board and, where required by the supervisor, share results with the supervisor.

58. The board should maintain appropriate records (eg meeting minutes or summaries of matters reviewed, recommendations made and decisions taken) of its deliberations and decisions. These should be made available to the supervisor when required.

Role of the chair

59. The chair of the board plays a crucial role in the proper functioning of the board. The chair provides leadership to the board and is responsible for its effective overall functioning, including maintaining a relationship of trust with board members. The chair should possess the requisite experience, competencies and personal qualities in order to fulfil these responsibilities. The chair should ensure that board decisions are taken on a sound and well informed basis. The chair should encourage and promote critical discussion and ensure that dissenting views can be freely expressed and discussed within the decision-making process.

60. To promote checks and balances, the chair of the board should be a non-executive board member and not serve as chair of any board committee.

61. In jurisdictions where the chair is permitted to assume executive duties, the bank should have measures in place to mitigate the adverse impact on the bank's checks and balances of such a situation. These could include having a lead board member, senior independent board member or a similar position or having a larger number of non-executives on the board so as to provide effective challenge to executive board members.

Board committees

62. To increase efficiency and allow deeper focus in specific areas, a board may establish certain specialised board committees, unless it can demonstrate to the supervisor that it can still effectively accomplish the goals described below without such committees. The committees should be created and mandated by the full board. The number and nature of committees depends on many factors, including the size of the bank and its board, the nature of the business areas of the bank, and its risk profile.

63. Each committee should have a charter or other instrument that sets out its mandate, scope and working procedures. This includes how the committee will report to the full board, what is expected of committee members and any tenure limits for serving on the committee. The board should consider the occasional rotation of members and of the chair of such committees as this can help avoid undue concentration of power and promote fresh perspectives.

64. In the interest of greater transparency and accountability, a board should disclose the committees it has established, their mandates and their composition (including members who are considered to be independent).

65. Committees should maintain appropriate records of their deliberations and decisions (eg meeting minutes or summaries of matters reviewed, recommendations made and decisions taken). Such records should document the committees' fulfilment of their responsibilities and help the supervisor or those responsible to assess the effectiveness of these committees.

66. A committee chair should be an independent, non-executive board member.

Audit committee

67. The audit committee:[14]

- is required for systemically important banks. For banks of large size, risk profile or complexity it is strongly advised. For other banks it remains strongly recommended.
- is required to be distinct from other committees.
- should have a chair who is independent and is not the chair of the board or any other committee.
- should be made up entirely of independent or non-executive board members.
- should include members who have experience in audit practices and financial literacy at banks.

68. The audit committee is responsible, among other things, for:

- the financial reporting process;
- providing oversight of and interacting with the bank's internal and external auditors;
- approving, or recommending to the board or shareholders for their approval, the appointment[15] compensation and dismissal of external auditors;
- reviewing and approving the audit scope and frequency;

[14] See BCBS, *External audits of banks*, 2014, www.bis.org/publ/bcbs280.pdf.

[15] In some jurisdictions, external auditors are appointed directly by shareholders, with the board only making a recommendation.

- receiving key audit reports and ensuring that senior management 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 and other control functions;
- overseeing the establishment of accounting policies and practices by the bank; and
- reviewing the third-party opinions on the design and effectiveness of the overall risk governance framework and internal control system.

69. At a minimum, the audit committee as a whole should possess a collective balance of skills and expert knowledge – commensurate with the complexity of the banking organisation and the duties to be performed – and should have relevant experience in financial reporting, accounting and auditing. Where needed, the audit committee has access to external expert advice.

Risk committee

70. The risk committee of the board:

- is required for systemically important banks. For banks of large size, risk profile or complexity it is strongly advised. For other banks it remains strongly recommended.
- should be distinct from the audit committee, but may have other related tasks, such as finance.
- should have a chair who is an independent director and not the chair of the board, or any other committee.
- should include a majority of members who are independent.
- should include members who have experience in risk management issues and practices.
- should discuss all risk strategies on both an aggregated basis and by type of risk and make recommendations to the board thereon, and on the risk appetite.
- is required to review the bank's risk policies at least annually.
- should oversee that management has in place processes to ensure the bank's adherence to the approved risk policies.

71. The risk committee of the board is responsible for advising the board on the bank's overall current and future risk appetite, overseeing senior management's implementation of the RAS, reporting on the state of risk culture in the bank, and interacting with and overseeing the CRO.

72. The committee's work includes oversight of the strategies for capital and liquidity management, as well as for all relevant risks of the bank, such as credit, market, operational, compliance and reputational risks, to ensure they are consistent with the stated risk appetite.

73. The committee should receive regular reporting and communication from the CRO and other relevant functions about the bank's current risk profile, current state of the risk culture, utilisation against the established risk appetite and limits, limit breaches and mitigation plans (see Principle 6).

74. The risk committee should meet periodically with the audit and other risk-relevant committees to ensure effective exchange of information and effective coverage of all risks, including emerging risks and any needed adjustments to the risk governance framework of the bank in the light of its business plans and the external environment.

Compensation committee

75. The compensation committee is required for systemically important banks. It should oversee the compensation system's design and operation and ensure that compensation is appropriate and

consistent with the bank's culture, long-term business and risk appetite, performance and control environment (see Principle 10), as well as with any legal or regulatory requirements. The compensation committee should be constituted in a way that enables it to exercise competent and independent judgment on compensation policies and practices and the incentives they create. The compensation committee works closely with the bank's risk committee in evaluating the incentives created by the compensation system.

Other board committees

76. Among other specialised committees that have become increasingly common are the following:

- *Nominations/human resources/governance committee*: provides recommendations to the board for new board members and members of senior management; may be involved in assessment of board and senior management effectiveness; may be involved in overseeing the bank's personnel or human resource policies (see Principle 2).
- *Ethics/compliance committee*: ensures that the bank has the appropriate means for promoting proper decision-making and compliance with laws, regulations and internal rules; provides oversight of the compliance function.

77. The board should appoint members to specialised committees with the goal of achieving an optimal mix of skills and experience that, in combination, allow the committees to fully understand, objectively evaluate and bring fresh thinking to the relevant issues.

78. In jurisdictions permitting or requiring executive members on the board, the board of a bank should work to ensure the needed objectivity in each committee, such as by having only non-executives and, to the extent possible, a majority of independent members.

Conflicts of interest

79. Conflicts of interest may arise as a result of the various activities and roles of the bank (eg where the bank extends loans to a firm while its proprietary trading function buys and sells securities issued by that firm), or between the interests of the bank or its customers and those of the bank's board members or senior managers (eg where the bank enters into a business relationship with an entity in which one of the bank's board members has a financial interest).

80. Conflicts of interest may also arise when a bank is part of a broader group. For example, where the bank is part of a group, reporting lines and information flows between the bank, its parent company and/or other subsidiaries can lead to the emergence of conflicts of interest (eg sharing of potential proprietary, confidential or otherwise sensitive information from different entities or pressure to conduct business on a non-arm's length basis).

81. The board should ensure that policies to identify potential conflicts of interest are developed, implemented and monitored. Where these conflicts cannot be prevented, they should be properly managed (based on the permissibility of relationships or transactions under sound corporate policies consistent with national law and supervisory standards).

82. The board should have a formal written conflicts of interest policy and an objective compliance process for implementing the policy. The policy should include:

- a member's duty to avoid to the extent possible activities that could create conflicts of interest or the appearance of conflicts of interest;
- examples of where conflicts can arise when serving as a board member;

- a rigorous review and approval process for members to follow before they engage in certain activities (such as serving on another board) so as to ensure that such activity will not create a conflict of interest;[16]
- a member's duty to promptly disclose any matter that may result, or has already resulted, in a conflict of interest;
- a member's responsibility to abstain from voting on any matter where the member may have a conflict of interest or where the member's objectivity or ability to properly fulfil duties to the bank may be otherwise compromised;
- adequate procedures for transactions with related parties so that they be made on an arm's length basis; and
- the way in which the board will deal with any non-compliance with the policy.

83. The board should ensure that appropriate public disclosure is made, and/or information is provided to supervisors, relating to the bank's policies on conflicts of interest and potential material conflicts of interest.

84. This should include information on the bank's approach to disclosing and managing material conflicts of interest that are not consistent with such policies, and conflicts that could arise because of the bank's affiliation or transactions with other entities within the group.

85. There is a potential conflict of interest where a bank is both owned by the state and subject to banking supervision by the state. If such conflicts of interest do exist, there should be full administrative separation of the ownership and banking supervision functions in order to minimise political interference in the supervision of the bank.

[16] For example, one done by at least two members of the board or by a committee of the board, or done with the involvement of one of the risk management, compliance or internal audit functions or with the help of an independent external expert.

Principle 4: Senior management

Under the direction and oversight of the board, senior management should carry out and manage the bank's activities in a manner consistent with the business strategy, risk appetite, incentive compensation and other policies approved by the board.

86. Senior management consists of a core group of individuals who are responsible and accountable to the board for effectively overseeing the day-to-day management of the bank.

87. The organisation and procedures and decision-making of senior management should be clear and transparent and designed to promote effective management of the bank. This includes clarity on the role and authority of the various positions within senior management, including the CEO.

88. Members of senior management should have the necessary experience, competencies and integrity to manage the businesses and people under their supervision. They should receive access to regular training to maintain and enhance their competencies and stay up to date on developments relevant to their areas of responsibility.

89. Members of senior management should be selected through an appropriate promotion or recruitment process which takes into account the qualifications required for the position in question. For those senior management positions for which the board of directors is required to review or select candidates through an interview process, senior management should provide sufficient information to the board.

90. Senior management contributes substantially to a bank's sound corporate governance through personal conduct (eg by helping to set the "tone at the top" along with the board). Members of senior management should provide adequate oversight of those they manage, and ensure that the bank's activities are consistent with the business strategy, risk appetite and the policies approved by the board.

91. Senior management is responsible for delegating duties to staff and should establish a management structure that promotes accountability and transparency throughout the bank.

92. Senior management should implement, consistent with the direction given by the board, risk management systems, processes and controls for managing the risks – both financial and non-financial – to which the bank is exposed and for complying with laws, regulations and internal policies.

- This includes comprehensive and independent risk management, compliance and audit functions, as well as an effective overall system of internal controls.
- Senior management should recognise and respect the independent duties of the risk management, compliance and internal audit functions and should not interfere in their exercise of such duties.

93. Senior management should provide the board with the information it needs to carry out its responsibilities, supervise senior management and assess the quality of senior management's performance. In this regard, senior management should keep the board regularly and adequately informed of material matters, including:

- changes in business strategy, risk strategy/risk appetite;
- bank performance and condition;
- breaches of risk limits or compliance rules;
- internal control failures; and
- legal or regulatory concerns.

Principle 5: Governance of group structures

In a group structure, the board of the parent company has the overall responsibility for the group and for ensuring that there is a clear governance framework appropriate to the structure, business and risks of the group and its entities.[17] The board and senior management should know and understand the bank's operational structure and the risks that it poses.

Parent company boards

94. In operating within a group structure, the board of the parent company should be aware of the material risks and issues that might affect both the bank as a whole and its subsidiaries. It should exercise adequate oversight over subsidiaries while respecting the independent legal and governance responsibilities that might apply to subsidiary boards.

95. In order to fulfil its responsibilities, the board of the parent company should:

- establish a group structure (including the legal entity and business structure) and a governance framework with clearly defined roles and responsibilities, including those at the parent company level and those at the subsidiary level;
- define an appropriate subsidiary board and management structure to contribute to the effective oversight of businesses and subsidiaries, which takes into account the different risks to which the group, its businesses and its subsidiaries are exposed;
- assess whether the group's corporate governance framework includes adequate policies, processes and controls and addresses risks across the business and legal entity structures;
- ensure the group's corporate governance framework includes appropriate processes and controls to identify and address potential intragroup conflicts of interest, such as those arising from intragroup transactions;
- approve policies and clear strategies for establishing new structures and legal entities, and ensure that they are consistent with the policies and interests of the group;
- assess whether there are effective systems in place to facilitate the exchange of information among the various entities, to manage the risks of the separate entities as well as of the group as a whole, and to ensure effective supervision of the group;
- have sufficient resources to monitor compliance of subsidiaries with all applicable legal, regulatory and governance requirements; and
- maintain an effective relationship with both the home regulator and, through the subsidiary board or direct contact, with the regulators of all subsidiaries.

[17] Banks that are part of a conglomerate should also take into account the Joint Forum's *Principles for the supervision of financial conglomerates* (September 2013, www.bis.org/publ/joint29.htm). For purposes of the corporate governance principles herein, "parent company" and "group" refer to a financial group.

Subsidiary boards

96. While the strategic objectives, risk governance framework, corporate values and corporate governance principles of the subsidiary bank should align with that of the parent company (referred to here as "group policies"), the subsidiary board should make necessary adjustments where a group policy conflicts with an applicable legal or regulatory provision or prudential rule, or would be detrimental to the sound and prudent management of the subsidiary.

97. In the case of a significant regulated subsidiary (due to its risk profile or systemic importance or due to its size relative to the parent company), the board of the significant subsidiary should take such further steps as are necessary to help the subsidiary meet its independent corporate governance responsibilities and the legal and regulatory requirements that apply to it.

Complex or opaque structures

98. Banks create structures for legal, regulatory and tax purposes. Structures can take the form of units, branches, subsidiaries or other legal entities that can considerably increase the complexity of the organisation. The number of legal entities, and in particular the interconnections and intragroup transactions among such entities, can lead to challenges in identifying and managing the risks of the organisation as a whole.

99. Operating through complex or non-transparent structures may pose financial, legal, reputational and other risks to the bank. It may impede the ability of the board and senior management to conduct appropriate business oversight and could hinder effective banking supervision. In addition, the bank may also be indirectly exposed to risk when it performs certain services or establishes structures on behalf of customers.[18] Examples include acting as a company or partnership formation agent, providing a range of trustee services and developing complex structured finance transactions for customers. While these activities are often profitable and can serve the legitimate business purposes of customers, customers may in some cases use products and activities provided by banks to engage in illegal or inappropriate activities.

100. Senior management, and the board as appropriate, should be cognisant of these challenges and take appropriate action to avoid or mitigate them by:

- avoiding setting up unnecessarily complicated structures or an inordinate number of legal entities.
- continually maintaining and reviewing appropriate policies, procedures and processes governing the approval and maintenance of those structures or activities, including fully vetting the purpose, the associated risks and the bank's ability to manage those risks prior to setting up new structures and initiating associated activities.
- having a centralised process for approving the creation of new legal entities based on established criteria, including the ability to monitor and fulfil each entity's regulatory, tax, financial reporting, governance and other requirements.
- establishing adequate procedures and processes to identify and manage all material risks arising from these structures, including lack of management transparency, operational risks introduced by interconnected and complex funding structures, intragroup exposures, trapped

[18] See BCBS, *Customer due diligence for banks*, October 2001, www.bis.org/publ/bcbs85.htm.

collateral and counterparty risk. The bank should only approve structures if the material risks can be properly identified, assessed and managed.

- ensure that the activities and structure are subject to regular internal and external audit reviews.

101. The board of the parent company can enhance the effectiveness of the above efforts by requiring a periodic independent formal review of the structures, their controls and activities, as well as their consistency with board-approved strategy.

102. The board should be prepared to discuss with, and as necessary report to, the bank's supervisor and the host country supervisors the policies and strategies adopted regarding the establishment and maintenance of these structures and activities.

Principle 6: Risk management

Banks should have an effective independent risk management function, under the direction of a Chief Risk Officer (CRO), with sufficient stature, independence, resources and access to the board.

103. The independent risk management function is a key component of the bank's second line of defence. This function is responsible for overseeing risk-taking activities across the enterprise. The independent risk management function (bank-wide and within subsidiaries) should have authority within the organisation to oversee the bank's risk management activities. Key activities of the risk management function should include:

- identifying material individual, aggregate and emerging risks;
- assessing these risks and measuring the bank's exposure to them;
- supporting the board in its implementation, review and approval of the enterprise-wide risk governance framework which includes the bank's risk culture, risk appetite, RAS and risk limits;
- ongoing monitoring of the risk-taking activities and risk exposures to ensure they are in line with the board-approved risk appetite, risk limits and corresponding capital or liquidity needs (ie capital planning);
- establishing an early warning or trigger system for breaches of the bank's risk appetite or limits;
- influencing and, when necessary, challenging material risk decisions; and
- reporting to senior management and the board or risk committee, as appropriate, on all these items, including but not limited to proposing appropriate risk-mitigating actions.

104. While it is common for risk managers to work closely with individual business units, the risk management function should be sufficiently independent of the business units and should not be involved in revenue generation. Such independence is an essential component of an effective risk management function, as is having access to all business lines that have the potential to generate material risk to the bank as well as to relevant risk-bearing subsidiaries and affiliates.

105. The risk management function should have a sufficient number of personnel who possess the requisite experience and qualifications, including market and product knowledge as well as command of risk disciplines.[19] Staff should have the ability and willingness to effectively challenge business lines regarding all aspects of risk arising from the bank's activities.

Role of the CRO

106. Large, complex and internationally active banks, and other banks, based on their risk profile and local governance requirements, should have a senior manager (CRO or equivalent) with overall responsibility for the bank's risk management function. In banking groups, there should be a group CRO in addition to subsidiary-level risk officers. Because some banks may have an officer who fulfils the function of a CRO under a different title, reference in this document to the CRO is intended to

[19] Some banks have found it to be a sound practice to encourage or require staff to gain experience in both business line and risk management roles, on a rotational basis. Such an approach can have several benefits, including giving risk management stature within the bank commensurate with business lines and other functions, promoting bank-wide dialogue regarding risk, and ensuring that business lines understand the importance of risk management and that risk managers understand how business lines operate.

incorporate equivalent positions, provided they meet the independence and other requirements set out herein.

107. The CRO has primary responsibility for overseeing the development and implementation of the bank's risk management function. The CRO is responsible for supporting the board in its development of the bank's risk appetite and RAS and for translating the risk appetite into a risk limits structure. The CRO, together with management, should be actively engaged in the process of setting risk measures and limits for the various business lines and monitoring their performance relative to risk-taking and limit adherence. The CRO's responsibilities also include managing and participating in key decision-making processes (eg strategic planning, capital and liquidity planning, new products and services, compensation design and operation).

108. The CRO should have the organisational stature, authority and the necessary skills to oversee the bank's risk management activities. The CRO should be independent and have duties distinct from other executive functions. This requires the CRO to have access to any information necessary to perform his or her duties. The CRO, however, should not have management or financial responsibility related to any operational business lines or revenue-generating functions and there should be no "dual hatting" (ie the chief operating officer, CFO, chief auditor or other senior manager should in principle not also serve as the CRO).[20] While formal reporting lines may vary across banks, the CRO should report and have direct access to the board or its risk committee without impediment. The CRO should have the ability to engage with the board and with senior management on key risk issues. Interaction between the CRO and the board and/or risk committee should occur regularly, and the CRO should have the ability to meet with the board or risk committee without executive directors being present.

109. Appointment, dismissal and other changes to the CRO position should be approved by the board or its risk committee. If the CRO is removed from his or her position, this should be disclosed publicly. The bank should also discuss the reasons for such removal with its supervisor. The CRO's performance, compensation and budget should be reviewed and approved by the risk committee or the board.

[20] Where such "dual hatting" is unavoidable (eg in smaller institutions where resource constraints may make overlapping responsibilities necessary), these roles should be compatible – for example, the CRO may also have lead responsibility for a particular risk area – and should not weaken checks and balances within the banks.

Principle 7: Risk identification, monitoring and controlling

Risks should be identified, monitored and controlled on an ongoing bank-wide and individual entity basis. The sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, to the external risk landscape and in industry practice.

110. The bank's risk governance framework should include policies, supported by appropriate control procedures and processes, designed to ensure that the bank's risk identification, aggregation, mitigation and monitoring capabilities are commensurate with the bank's size, complexity and risk profile.

111. Risk identification should encompass all material risks to the bank, on- and off-balance sheet and on a group-wide, portfolio-wise and business-line level. In order to perform effective risk assessments, the board and senior management, including the CRO, should, regularly and on an ad hoc basis, evaluate the risks faced by the bank and its overall risk profile. The risk assessment process should include ongoing analysis of existing risks as well as the identification of new or emerging risks. Risks should be captured from all organisational units that originate risk. Concentrations associated with material risks shall likewise be factored into the risk assessment.

112. Risk identification and measurement should include both quantitative and qualitative elements. Risk measurements should also include qualitative, bank-wide views of risk relative to the bank's external operating environment. Banks should also have a method to identify and measure hard-to-quantify risks, such as reputation risk.

113. Internal controls are designed, among other things, to ensure that each key risk has a policy, process or other measure, as well as a control to ensure that such policy, process or other measure is being applied and works as intended. As such, internal controls help ensure process integrity, compliance and effectiveness. Internal controls provide reasonable assurance that financial and management information is reliable, timely and complete and that the bank is in compliance with its various policies and applicable laws and regulations.

114. In order to avoid actions beyond the authority of the individual or even fraud, internal controls also place reasonable checks on managerial and employee discretion. Even in smaller banks, for example, key management decisions should be taken by more than one person. Internal reviews should also determine the extent of a bank's compliance with company policies and procedures, as well as with legal and regulatory policies. Adequate escalation procedures are a key element of the internal control system.

115. The sophistication of the bank's risk management infrastructure including, in particular, a sufficiently robust data, data architecture and information technology infrastructure – should keep pace with developments such as balance sheet and revenue growth; increasing complexity of the bank's business, risk configuration or operating structure; geographic expansion; mergers and acquisitions; or the introduction of new products or business lines.

116. Banks must have accurate internal and external data to identify and assess risk, make strategic business decisions and determine capital and liquidity adequacy. The board and senior management should give special attention to the quality, completeness and accuracy of the data used to make risk

decisions.[21] While tools such as external credit ratings or externally purchased risk models and data can be useful as inputs into a more comprehensive assessment, banks ultimately are responsible for the assessment of their risks.

117. Risk measurement and modelling techniques should be used in addition to, but should not replace, qualitative risk analysis and monitoring. The risk management function should keep the board and senior management apprised of the assumptions used in and potential shortcomings of the bank's risk models and analyses. This helps ensure more complete and accurate reflection of exposures and may allow quicker action to address and mitigate risks.

118. As part of its quantitative and qualitative analysis, the bank should utilise stress tests and scenario analyses to better understand potential risk exposures under a variety of adverse circumstances.[22]

- Internal stress tests should cover a range of scenarios based on reasonable assumptions regarding dependencies and correlations. Senior management and, as applicable, the board should review and approve the scenarios that are used in the bank's risk analyses.
- Stress test programme results should be periodically reviewed with the board or its risk committee. Test results should be incorporated into the reviews of the risk appetite, the capital adequacy assessment process, the capital and liquidity planning processes, and budgets. They should also be linked to recovery and resolution planning. The risk management function should suggest if and what action is required based on results.
- The results of stress tests and scenario analyses should also be communicated to, and given appropriate consideration by, relevant business lines and individuals within the bank.

119. Banks should regularly compare actual performance against risk estimates (ie backtesting) to assist in judging the accuracy and effectiveness of the risk management process and making necessary adjustments.

120. In addition to identifying and measuring risk exposures, the risk management function should evaluate possible ways to mitigate these exposures. In some cases, the risk management function may direct that risk be reduced or hedged to limit exposure. In other cases, such as when there is a decision to accept or take risk that is beyond risk limits (ie on a temporary basis) or take risk that cannot be hedged or mitigated, the risk management function should report and monitor the positions to ensure that they remain within the bank's framework of limits and controls or within exception approval. Either approach may be appropriate depending on the issue at hand, provided that the independence of the risk management function is not compromised.

121. Banks should have risk management and approval processes for new or expanded products or services, lines of business and markets, as well as for large and complex transactions that require significant use of resources or have hard-to-quantify risks. Banks should also have review and approval processes for outsourcing bank functions to third parties. The risk management function should provide input on risks as part of such processes and on the outsourcer's ability to manage risks and comply with legal and regulatory obligations. Such processes should include:

[21] See BCBS, *Principles for effective risk data aggregation and risk reporting,* January 2013 including its progress report of December 2013.

[22] See BCBS, *Principles for sound stress testing practices and supervision*, May 2009, www.bis.org/publ/bcbs155.htm.

- A full and frank assessment of risks under a variety of scenarios, as well as an assessment of potential shortcomings in the ability of the bank's risk management and internal controls to effectively manage associated risks.
- An assessment of the extent to which the bank's risk management, legal and regulatory compliance, information technology, business line and internal control functions have adequate tools and the expertise necessary to measure and manage related risks.
- If adequate risk management processes are not in place, a new product, service, business line or third-party relationship or major transaction should be delayed until the bank is able to appropriately address the activity.
- There should also be a process to assess risk and performance relative to initial projections and to adapt the risk management treatment accordingly as the business matures.

122. Effective risk identification and measurement approaches are likewise necessary in subsidiary banks and affiliates.[23] Material risk-bearing affiliates and subsidiaries should be captured by the bank-wide risk management system and should be a part of the overall risk governance framework.[24]

123. Subsidiary boards and senior management remain responsible for developing effective risk management processes for their entities. The methods and procedures applied by subsidiaries should support the effectiveness of risk management at a group level. While parent companies should conduct strategic, group-wide risk management and prescribe corporate risk policies, subsidiary management and boards should have appropriate input to their local or regional application and to the assessment of local risks. Parent companies should ensure that adequate tools and authorities are available to the subsidiary and that the subsidiary understands what reporting obligations it has to the head office.

124. Mergers and acquisitions, divestitures and other changes to a bank's organisational structure can pose special risk management challenges to the bank. In particular, risks can arise from conducting insufficient due diligence that fails to identify post-merger risks or activities conflicting with the bank's strategic objectives or risk appetite. The risk management function should be actively involved in assessing risks that could arise from mergers and acquisitions and report its findings directly to the board or its risk committee.

[23] However, there may be national laws that exempt subsidiaries from some supervisory requirements on a standalone basis if these subsidiaries are well integrated in a group and a number of preconditions are met. The considerations set out in this paragraph apply in circumstances where no such exception is available.

[24] The risk governance framework should also cover the relevant risk-bearing affiliates of the group to ensure that the policies, business strategies, processes and controls of the affiliates are in broad alignment with the group's objectives.

Principle 8: Risk communication

An effective risk governance framework requires robust communication within the bank about risk, both across the organisation and through reporting to the board and senior management.

125. Ongoing communication about risk issues, including the bank's risk strategy, throughout the bank is a key tenet of a strong risk culture. A strong risk culture should promote risk awareness and encourage open communication and challenge about risk-taking across the organisation as well as vertically to and from the board and senior management. Senior management should keep control functions informed of management's major plans and activities so that the control functions can properly assess the risks.

126. Information should be communicated to the board and senior management in a timely, accurate and understandable manner so that they are equipped to take informed decisions. While ensuring that the board and senior management are sufficiently informed, management and those responsible for the risk management function should avoid voluminous information that can make it difficult to identify key issues. Rather, information should be prioritised and presented in a concise, fully contextualised manner. The board should institute periodic reviews of the relevance and accuracy of information it receives and determine if additional information is needed.

127. Material risk-related ad hoc information that requires immediate decisions or reactions should be promptly presented to senior management and the board, the responsible officers and, where applicable, the heads of control functions, so that suitable measures and activities can be initiated at an early stage. Suitable policies and procedures should be established for this purpose.

128. Risk reporting to the board requires careful design in order to ensure that bank-wide, individual portfolio and other risks are conveyed in a concise and meaningful manner. Reporting should accurately communicate risk exposures and results of stress tests or scenario analyses and should provoke a robust discussion of, for example, the bank's current and prospective exposures (particularly under stressed scenarios), risk/return relationships and risk appetite and limits. Reporting should also include information about the external environment to identify market conditions and trends that may have an impact on the bank's current or future risk profile.

129. Risk reporting systems should be dynamic, comprehensive and accurate, and should draw on a range of underlying assumptions. Risk monitoring and reporting should not only occur at the disaggregated level (including risk residing in subsidiaries that could be considered significant), but should also be aggregated to allow for a bank-wide or integrated perspective of risk exposures. Risk reporting systems should be clear about any deficiencies or limitations in risk estimates, as well as any significant embedded assumptions (eg regarding risk dependencies or correlations).

130. Banks should avoid organisational "silos" that can impede effective sharing of information across an organisation and can result in decisions being taken in isolation from the rest of the bank.[25] Overcoming these information-sharing obstacles may require the board, senior management and control functions to re-evaluate established practices in order to encourage greater communication.

[25] Organisational silos can be characterised by business lines, legal entities and/or geographic units being run in isolation from each other, with limited information shared and, in some cases, competition across silos.

Principle 9: Compliance

The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance approach and policies, including the establishment of a permanent compliance function.

131. An independent compliance function[26] is a key component of the bank's second line of defence. This function is responsible, among other things, for promoting and monitoring that the bank operates with integrity and in compliance with applicable, laws, regulations and internal policies.

132. Compliance starts at the top. It will be most effective in a corporate culture that emphasises standards of honesty and integrity and in which the board of directors and senior management lead by example. It concerns everyone within the bank and should be viewed as an integral part of the bank's business activities. A bank should hold itself to high standards when carrying out its business and should at all times strive to observe the spirit as well as the letter of the law. Failure to consider the impact of its actions on its shareholders, customers, employees and the markets may result in significant adverse publicity and reputational damage, even if no law has been broken.

133. The bank's senior management is responsible for establishing a written compliance approach and policies that contain the basic principles to be followed by the board, management and staff, and explains the main processes by which compliance risks are to be identified and managed through all levels of the organisation. Clarity and transparency may be promoted by making a distinction between general standards for all staff members and rules that only apply to specific groups of staff.

134. While the board and management are accountable for the bank's compliance, the compliance function has an important role in supporting corporate values, policies and processes that help ensure that the bank acts responsibly and observes all obligations applicable to it.

135. The compliance function should advise the board and senior management on compliance laws, rules and standards, including keeping them informed of developments in the area. It should also help educate staff about compliance issues, act as a contact point within the bank for compliance queries from staff members, and provide guidance to staff on the appropriate implementation of compliance laws, rules and standards in the form of policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

136. The compliance function is independent from management and provides separate reporting to the board on the bank's efforts in the above areas and on how the bank is managing its compliance risk.

137. To be effective, the compliance function must have sufficient authority, stature, independence, resources and access to the board. Management should respect the independent duties of the compliance function and not interfere with them.

138. The areas of special focus by the compliance function include those that could create reputational risk for the bank, including bribery, money laundering, country sanctions, fair treatment of the consumer and practices raising ethical issues.

[26] See BCBS, *Compliance and the compliance function in banks*, 2005, www.bis.org/publ/bcbs113.pdf.

Principle 10: Internal audit

The internal audit function provides independent assurance to the board and supports board and senior management in promoting an effective governance process and the long-term soundness of the bank. The internal audit function should have a clear mandate, be accountable to the board, be independent of the audited activities and have sufficient standing, skills, resources and authority within the bank.

139. The board and senior management should recognise and acknowledge that an independent and qualified internal audit function is vital to an effective governance process.

140. An effective internal audit function provides an independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation.[27]

141. The internal audit function should be accountable to the board on all matters related to the performance of its mandate as described in the internal audit charter. It must be independent of the audited activities and have sufficient standing, authority and resources within the bank to enable the auditors to carry out their assignments effectively and objectively.

142. The board and senior management can enhance the effectiveness of the internal audit function by:

- requiring the function to independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes;
- requiring internal auditors to adhere to national and international professional standards, such as those established by the Institute of Internal Auditors; and
- ensuring that audit staff have skills and resources commensurate with the business activities and risks of the bank.

143. The board and senior management should respect and promote the independence of the internal audit function by, for example:

- ensuring that internal audit reports are provided to the board without management filtering and that the internal auditors have direct access to the board or the board's audit committee.
- requiring timely and effective correction of audit issues by senior management.
- requiring a periodic assessment of the bank's overall risk governance framework including, but not limited to, an assessment of:
    - the effectiveness of the risk management and compliance functions;
    - the quality of risk reporting to the board and senior management; and
    - the effectiveness of the bank's system of internal controls.

[27] See BCBS, *The internal audit function in banks*, 2012, www.bis.org/publ/bcbs223.pdf.

Principle 11: Compensation

The bank's compensation structure should be effectively aligned with sound risk management and should promote long term health of the organisation and appropriate risk-taking behaviour.

144. Compensation systems form a key component of the governance and incentive structure through which the board and senior management promote good performance, convey acceptable risk-taking behaviour and reinforce the bank's operating and risk culture. The board is responsible for the overall oversight of the compensation system for the entire bank. In addition, the board should regularly monitor and review outcomes to ensure that the bank-wide compensation system is operating as intended.[28] The board should review the compensation policy at least annually.

145. The FSB principles on compensation are intended to apply to significant financial institutions but they are especially critical for large, systemically important firms. National jurisdictions may also apply the principles in a proportionate manner to smaller, less complex institutions. Banks are encouraged to implement the FSB principles, or consistent national provisions based on them.

146. The board should approve the compensation of senior executives, including the CEO, CRO and the head of internal audit, and should oversee management's development and operation of compensation policies, systems and related control processes.

147. Significant financial institutions should have a board remuneration committee as an integral part of their governance structure and organisation to oversee the compensation system's design and operation on behalf of the board of directors. The remuneration committee should be constituted in a way that enables it to exercise competent and independent judgment on compensation policies and practices and the incentives created for managing risk, capital and liquidity.

148. For employees in risk, compliance and other control functions, compensation should be determined independently of any business line overseen, and performance measures should be based principally on the achievement of their own objectives so as not to compromise their independence.

149. The compensation structure should promote long term performance and be in line with the business and risk strategy, objectives, values and long-term interests of the bank and incorporate measures to prevent conflicts of interests. Compensation programmes should facilitate adherence to risk appetite, promote appropriate risk-taking behaviour and encourage employees to act in the interest of the company as a whole (also taking into account client interests) rather than for themselves or only their business lines.

150. Practices by which compensation is paid for potential future revenues whose timing and likelihood remain uncertain should be carefully evaluated by means of both qualitative and quantitative key indicators. Banks should ensure that variable compensation is adjusted to take into account the full range of current and potential risks an employee takes as well as realised risks, including breaches of internal procedures or legal requirements. Compensation should reflect risk-taking and risk outcomes.

151. Compensation payout schedules should be sensitive to risk outcomes over a multi-year horizon. This is often achieved through arrangements that defer a sufficiently large part of the compensation for a sufficiently long period of time until risk outcomes become better known. This includes "malus/forfeiture" provisions (where compensation can be reduced or reversed based on realised risks or

[28] By implementing the *FSB Principles for Sound Compensation Practices* and their *Implementation Standards – Second progress report*, 26 August 2013, p 14.

conduct events before compensation vests) and/or "clawback" provisions under which compensation can be reduced or reversed after compensation vests if new facts emerge that the compensation paid was based on erroneous assumptions (such as misreporting) or if it is discovered that the employee has failed to comply with internal policies or legal requirements. "Golden hellos" or "golden parachutes" under which new or terminated executives or staff receive large payouts irrespective of performance are generally not consistent with sound compensation practice.

Principle 12: Disclosure and transparency

The governance of the bank should be adequately transparent to its shareholders, depositors, other relevant stakeholders and market participants.

152. Transparency is consistent with sound and effective corporate governance. As emphasised in existing Committee guidance on bank transparency,[29] it is difficult for shareholders, depositors, other relevant stakeholders and market participants to effectively monitor and properly hold the board and senior management accountable when there is insufficient transparency. The objective of transparency in the area of corporate governance is therefore to provide these parties with the information necessary to enable them to assess the effectiveness of the board and senior management in governing the bank.

153. Although disclosure may be less detailed for non-listed banks, especially those that are wholly owned, these banks can nevertheless pose the same types of risk to the financial system as publicly traded banks through various activities, including their participation in payment systems and acceptance of retail deposits.

154. All banks, even those for whom disclosure requirements may differ because they are non-listed, should disclose relevant and useful information that supports the key areas of corporate governance identified by the Committee. Such disclosure should be proportionate to the size, complexity, structure, economic significance and risk profile of the bank. At a minimum, banks should disclose annually the following information:

- the recruitment approach for the selection of members of the board and their knowledge, skills and expertise;
- the policy for ensuring board membership that represents appropriate diverse views, its objectives and the extent to which these objectives have been achieved; and
- whether the bank has set up board committees and the number of times these committees have met.

155. In general, the bank should apply the disclosure and transparency section of the OECD principles.[30] Accordingly, disclosure should include, but not be limited to, material information on the bank's objectives, organisational and governance structures and policies (in particular the content of any corporate governance or remuneration code or policy and the process by which it is implemented), major share ownership and voting rights and related party transactions. Relevant banks should appropriately disclose their incentive and compensation policy following the FSB principles related to compensation. In particular, an annual report on compensation should be disclosed to the public. It should include: the decision-making process used to determine the bank-wide compensation policy; the most important design characteristics of the compensation system, including the criteria used for performance measurement and risk adjustment; and aggregate quantitative information on compensation.

[29] See BCBS, *Enhancing bank transparency*, September 1998, www.bis.org/publ/bcbs41.htm, and *Review of the Pillar 3 disclosure requirements*, June 2014, www.bis.org/publ/bcbs286.pdf; and FSB *Enhancing the risk disclosures of banks – report of the Enhanced Disclosure Task Force*, October 2012, www.financialstabilityboard.org/publications/r_121029.pdf.

[30] Section V of the OECD principles states, "The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company." See footnote 8 for reference.

156. The bank should also disclose key points concerning its risk exposures and risk management strategies without breaching necessary confidentiality. When involved in complex or non-transparent activities, the bank should disclose adequate information on their purpose, strategies, structures, and related risks and controls.

157. Disclosure should be accurate, clear and presented such that shareholders, depositors, other relevant stakeholders and market participants can consult the information easily. Timely public disclosure is desirable on a bank's public website, in its annual and periodic financial reports, or by other appropriate means. It is good practice to have an annual corporate governance-specific and comprehensive statement in a clearly identifiable section of the annual report depending on the applicable financial reporting framework. All material developments that arise between regular reports should be disclosed to the bank supervisor and relevant stakeholders as required by law without undue delay.

Principle 13: The role of supervisors

Supervisors should provide guidance for and supervise corporate governance at banks, including through comprehensive evaluations and regular interaction with boards and senior management, should require improvement and remedial action as necessary, and should share information on corporate governance with other supervisors.

158. The board and senior management are primarily responsible for the governance of the bank, and shareholders and supervisors should hold them accountable for this. This section sets forth several principles that can assist supervisors in assessing corporate governance and fostering good corporate governance in banks.

Guidance on expectations for sound corporate governance

159. Supervisors should establish guidance or rules, consistent with the principles set forth in this document, requiring banks to have robust corporate governance policies and practices. Such guidance is especially important where national laws, regulations, codes or listing requirements regarding corporate governance are too generic or not sufficient to address the unique corporate governance needs of banks. Regulatory guidance should address, among other things, expectations for checks and balances and a clear allocation of responsibilities, accountability and transparency among the board and senior management and within the bank. In addition to guidance or rules, where appropriate, supervisors should also share industry best practices regarding corporate governance with the banks they supervise.

Comprehensive evaluations of a bank's corporate governance

160. Supervisors should have processes in place to fully evaluate a bank's corporate governance. Such evaluations may be conducted through regular reviews of written materials and reports, interviews with board members and bank personnel, examinations, self-assessments by the bank, and other types of on- and off-site monitoring. The evaluations should also include regular communication with a bank's board of directors, senior management and those responsible for the risk, compliance and internal audit functions and external auditors.[31]

161. Supervisors should evaluate whether the bank has in place effective mechanisms through which the board and senior management execute their respective oversight responsibilities. Supervisors should evaluate whether the board and senior management have processes in place for the oversight of the bank's strategic objectives including risk appetite, financial performance, capital adequacy, capital planning, liquidity, risk profile and risk culture, controls, compensation practices, and the selection and evaluation of management. Supervisors should focus particular attention on the oversight of the risk management, compliance and internal audit functions. This should include assessing the extent to which the board interacts with and meets with representatives of these functions. Supervisors should determine whether internal controls are being adequately assessed and contribute to sound governance throughout the bank.

162. Supervisors should evaluate the processes and criteria used by banks in the selection of board members and senior management and, as they judge necessary, obtain information about the expertise

[31] External auditors may share information with the supervisor without contravening their duty of confidentiality (see BCBS, *External audits of banks*, 2014 paragraphs 95 and 96).

and character of board members and senior management. The fit and proper criteria should include those discussed in Principle 2 of this document. The individual and collective suitability of board members and senior management should be subject to ongoing attention by supervisors.

163. As part of their evaluation of the overall corporate governance in a bank, supervisors should also endeavour to assess the governance effectiveness of the board and senior management, especially with respect to the risk culture of the bank. An assessment of governance effectiveness aims to determine the extent to which the board and senior management demonstrate effective behaviours that contribute to good governance. This includes consideration of the behavioural dynamic of the board and senior management, such as how the "tone at the top" and the cultural values of the bank are communicated and put into practice, how information flows to and from the board and senior management, and how potential serious problems are identified and addressed throughout the organisation. The evaluation of governance effectiveness includes review of any board and management assessments, surveys and other information often used by banks in assessing their internal culture, as well as supervisory observations and qualitative judgments. In arriving at such judgments, supervisors need to be particularly mindful of consistency of treatment across the banks they supervise and ensure that staff have appropriate training and competence in these areas.

164. In reviewing corporate governance in the context of a group structure, supervisors should take into account the corporate governance responsibilities of both the parent company and subsidiaries, in accordance with Principle 5 of this document.

Regular interaction with directors and senior management

165. Supervisors should interact regularly with boards of directors, individual board members, senior managers and those responsible for the risk management, compliance and internal audit functions. This should include scheduled meetings and ad hoc exchanges, through a variety of communication vehicles (eg e-mail, telephone, in-person meetings). The purpose of the interactions is to support timely and open dialogue between the bank and supervisors on a range of issues, including the bank's strategies, business model and risks, the effectiveness of corporate governance at the bank, the bank's culture, management issues and succession planning, compensation and incentives, and other supervisory concerns or expectations. Supervisors may also provide insights to the bank on its operations relative to its peers, market developments and emerging systemic risks.

166. The frequency of interactions with the above persons may vary according to the size, complexity, structure, economic significance and risk profile of the bank. On that basis, supervisors may, for example, meet with the full board of directors annually, but more frequently with the chairman or lead or senior independent director and with key committee chairs. For systemically important banks, interaction should occur more frequently, particularly with members of the board and members of senior management, and those responsible for risk management, compliance and internal audit functions.

Requiring improvement and remedial action by a bank

167. Supervisors should have a range of tools at their disposal to address governance improvement needs and governance failures. They should be able to require improvement steps and remedial action, and assure accountability for the corporate governance of a bank. These tools may include the ability to compel changes in the bank's policies and practices, the composition of the board of directors or senior management, or other corrective actions. They should also include, where necessary, the authority to impose sanctions or other punitive measures. The choice of tool and the time frame for any remedial action should be proportionate to the level of risk the deficiency poses to the safety and soundness of the bank or the relevant financial system(s).

168. When a supervisor requires a bank to take remedial action, the supervisor should set a timetable for completion. Supervisors should have escalation procedures in place to require more stringent or accelerated remedial action in the event that a bank does not adequately address the deficiencies identified or the supervisor deems that further action is warranted.

Cooperation and sharing of corporate governance information with other relevant supervisors

169. Cooperation and appropriate information-sharing among relevant public authorities, including bank supervisors, can significantly contribute to the effectiveness of these authorities in their respective roles. Such information-sharing is particularly important between home and host supervisors of cross-border banking entities.[32] Cooperation can occur on a bilateral basis, in the form of a supervisory college or through periodic meetings among supervisors at which corporate governance matters should be discussed. Such communication can help supervisors improve their assessment of the overall governance of a bank and the risks it faces, particularly in a group context, and help other authorities assess the risks posed to the broader financial system. Information shared should be relevant for supervisory purposes and be provided within the constraints of confidentiality and other applicable laws. Special arrangements, such as a memorandum of understanding, may be warranted to govern the sharing of information among supervisors or between supervisors and other authorities.

[32] See BCBS, *Core principles for effective supervision*, September 2012, www.bis.org/publ/bcbs230.pdf, Principle 13 (Home-host relationships).