BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Governance

Issued on: 1 March 2013

Issued on: 1 March 2013

PART A OVERVIEW

I. Introduction

1. The safety and soundness of financial institutions rely on the effectiveness of risk oversight and control functions. Over the last decade, risk management approaches and practices in the industry have evolved substantially, with increased attention to and advancements in risk management systems and practices observed among financial institutions. Despite such progress, scope remains for further improving internal risk governance practices which underpin a sound risk management framework. This includes closer integration within financial institutions of risk and corporate governance policies, processes and structures to support risk-related decision-making.

2. Risk governance focuses on applying the principles of sound corporate governance to the assessment and management of risks to ensure that risk-taking activities are aligned with an institution's capacity to absorb losses and its long-term viability. It is concerned in particular with the roles of the board, senior management, and risk management control functions as well as the processes by which risk information is collected, analysed and communicated to provide a sound basis for management decisions. It is also concerned with the effects of incentives and organisational culture on risk-taking behaviours and perceptions of risk in the institution. With increasingly complex business operations and activities, the availability of comprehensive and integrated systems to support an enterprise-wide or consolidated view of risks, for both the individual financial institution and for the group, is particularly critical. Also important is the capacity of institutions to respond swiftly to changes in the operating environment and developments in the institution's business strategies.

3. This policy document on Risk Governance sets out a framework of principles on risk governance to guide the board and senior management in performing their

risk oversight function. This policy document should be read jointly with the "Guidelines on Corporate Governance for Licensed Institutions" and for institutions with Islamic finance operations, the Guidelines on Shariah Governance for Islamic Financial Institutions. The overarching principles provided under this policy document are applicable to all financial institutions. Financial institutions are expected to apply these principles taking into account the size, complexity, risk profile and nature of their activities.

4. The principles in this policy document are foundation for and complement other guidelines and sound practices papers issued by the Bank on specific risks such as credit, market, operational, and liquidity risks. Collectively, they reflect the Bank's supervisory expectations with regards to financial institutions' risk management framework and practices, and form the basis for supervisory assessments of individual institutions performed by the Bank.

II. Scope of the Policy

5. This policy is applicable to all institutions licensed under the Banking and Financial Institutions Act 1989 (BAFIA), Islamic Banking Act 1983 (IBA), Insurance Act 1996 (IA), Takaful Act 1984 (TA), and Development Financial Institutions Act 2002 (DFIA), hereinafter referred to as financial institutions.

6. This policy is issued pursuant to Section 126 of the BAFIA, Section 53A of the IBA, Section 201 of the IA, Section 69 of the TA, and Section 126 of the DFIA.

PART B PRINCIPLES OF RISK GOVERNANCE

III. Board practices

Principle 1: The board must ensure that the financial institution's corporate objectives are supported by a sound risk strategy and an effective risk management framework that is appropriate to the nature, scale and complexity of its activities.

7. The board's overall responsibility for governing the financial institution and ensuring its long-term financial soundness includes determining the financial institution's business and risk strategies. The board must approve the financial institution's overall risk strategy[1], including the risk appetite[2] and oversee its implementation.

8. The financial institution's risk strategy should be directed by a clear risk appetite statement that is approved by the board and communicated throughout the organisation. The risk appetite must address the major types of risk that the institution needs to manage and the tolerance levels around specific risks that are acceptable to the institution in executing its business strategy. It should also reflect the risk preferences for the significant activities of the financial institution. The board must consider all relevant risks, including non-quantifiable risks.

9. The risk appetite statement should reflect the willingness and capacity of the institution to take on risk while taking a longer-term view that considers the institution's financial capacity, and continuing ability to meet obligations towards stakeholders, including, in particular, obligations to depositors and policyholders.

[1] Risk strategy is the plan to ensure that the business is operating within the financial institution's risk appetite.
[2] Risk appetite is a high level determination of how much risk a firm is willing to accept taking into account risk/return attributes.

The risk appetite should be consistent with the skills and resources available within the institution to manage and monitor risk exposures.

10. The board must take appropriate steps to ensure that business and operational decisions are aligned with the risk appetite set by the board. This includes reviewing management's implementation of an appropriate risk strategy and obtaining assurance that organisational units are operating within the parameters of the institution's appetite for specific types of risk. The board must also consider the institution's risk appetite when it approves management actions, including new product lines and business expansions and in assessing the remuneration policies and overall adequacy of capital[3] and liquidity buffers for the financial institution.

11. The risk appetite of the financial institution should guide strategy development and business plans (e.g. development of new products, ventures into new market or business activities, product pricing strategies, planning of technology, skills and resources required) and direct the institution's priorities for putting in place risk management tools and internal controls.

12. The board must review and affirm the institution's risk appetite regularly to ensure that it continues to be relevant and reflects any changes in the institution's capacity to take on risk, its inherent risk profile, as well as market and macroeconomic conditions.

13. The board must oversee the design and development of the risk management framework and ensure that the framework is effective for controlling risk-taking activities of the institution in line with the institution's risk appetite and has taken into account changes in the business environment. In doing so, the board should

[3] This principle should be read together with Risk-Weighted Capital Adequacy Framework (Basel II) – Internal Capital Adequacy Assessment Process (Pillar 2), Capital Adequacy for Islamic Banks (CAFIB) Internal Capital Adequacy Assessment Process (Pillar 2) and Guidelines on Internal Capital Adequacy Assessment Process for Insurers.

provide constructive challenge to management on the credibility and robustness of the framework to ensure that there are no material gaps or weaknesses.

14. The board must ensure that a sound control environment exists within the institution with clear identification of responsibilities for incurring and controlling risks assigned respectively to business units, the risk management and control functions, and internal audit. The board must ensure that all control functions and internal audit have the proper authority and are adequately staffed and resourced to carry out their responsibilities independently and effectively.

15. The board must be familiar with the operational structure of the financial institution and ensure that organisational complexity does not hamper effective enterprise-wide risk management in relation to the financial institution's activities (see Principles 11 and 12).

16. A consistent culture of risk awareness and risk management within the institution should be actively promoted by the board and senior management. A healthy risk culture should provide and reinforce appropriate norms and incentives for prudent risk-taking. The board should take the lead in establishing the tone-at-the-top and in upholding standards of conduct, organisational practices and corporate values that are consistent with the institution's overall risk appetite. This includes ensuring that risk managers actively participate and are engaged in discussions on strategic business issues. The corporate culture should also encourage regular and frank discussions on risk at various levels of the organisation and the timely communication of material risk developments across the organisation, including to senior management and the board, to support an enterprise-wide view of risk and promote the alignment of relevant risk mitigation activities.

Principle 2: The board must provide effective oversight of senior management's actions to ensure consistency with the risk strategy and policies approved by the board, including the risk appetite framework.

17. The board must establish appropriate internal oversight arrangements that would enable it to discharge its duties for effective risk oversight. This must include the establishment of a risk management committee of the board[4].

18. The board and its risk committee must regularly obtain information from senior management on adherence to the institution's risk appetite and the implementation of risk management policies, processes, and controls within the institution in managing the key risks to the institution as well as emerging risks. This should be supported by independent assessments by the risk management and control functions. The board and its risk committee should also provide constructive challenge to senior management and critically review the risk information and developments affecting the financial institution.

19. In ensuring the reliability of the information received by the board, the board must set clear expectations for senior management to ensure the integrity of the essential reporting and monitoring systems. This includes ensuring that the reporting structures do not distort or suppress material information to the board. Reporting processes should promote timely responses to material risk developments via clearly defined escalation triggers and procedures for significant risk events.

20. The board's risk committee and audit committee must also periodically meet to ensure effective exchange of information so as to enable effective coverage of all risks, including emerging risk issues that could have an impact on the institution's risk appetite and business plans.

[4] The roles and responsibilities of the board risk committee should be read together with the 'Risk Management Committee' section of the Bank's Guidelines on Corporate Governance for Licensed Institutions.

21. The board must collectively possess and maintain, including through continuing education and training, appropriate and sufficient knowledge and competencies in risk management to provide effective oversight and guidance to senior management on risk issues. The board must also require and ensure that senior management have the requisite skills, experience and competencies in risk management that are appropriate to the nature, scale and complexity of the financial institution's business.

22. The board and its risk committee should have the means and ability to seek independent third party views or information on risk implications as appropriate before coming to any conclusion or making any significant policy decisions. This should serve to promote informed and robust decision-making by the board in a manner that complements and adds value to the work of senior management.

IV. Senior management oversight

Principle 3: Senior management is responsible for ensuring that the day-to-day management of the financial institution's activities is consistent with the risk strategy, including the risk appetite, and policies approved by the board.

23. Senior management must establish clear guidance regarding the business and risk strategy, including risk limits, for individual operating units to ensure that risk-taking activities remain within the risk appetite for the overall institution. When new business strategies or activities are being pursued, senior management must ensure that all key risks associated with the activities have been identified and assessed to determine whether these risks are within the institution's risk appetite. In addition, senior management must contribute towards promoting a sound risk culture through a clear focus on risk in the activities of the institution and timely and proportionate responses to inappropriate risk-taking behaviour.

24. Senior management must establish and implement appropriate organisational structures and systems for managing financial and non-financial risks to which the financial institution is exposed. This includes the establishment of an effective risk management function that is independent from business units and an effective system of internal controls.

25. Senior management is responsible for establishing a management structure that promotes accountability and the effective oversight of delegated authority and responsibilities for risk-taking decisions. Reporting structures should promote adequate checks and balances such that deviations from the risk taking boundaries and parameters outlined by the board and senior management can be quickly identified and escalated to the appropriate level of management and the board as appropriate, for prompt corrective action.

V. Risk management and internal controls

Principle 4: The risk management framework must enable the identification, measurement, and continuous monitoring of all relevant and material risks on a group- and firm-wide basis, supported by robust management information systems that facilitate the timely and reliable reporting of risks and the integration of information across the institution. The sophistication of the financial institution's risk management framework must keep pace with any changes in the institution's risk profile (including its business growth and complexity) and the external risk environment.

26. Risk management approaches employed by financial institutions should take into consideration all relevant and material risks, capturing both quantitative and qualitative elements of risks. For Islamic banking and takaful operations, the risk management approaches and methodologies must be able to distinguish the different nature and combination of risks that are embedded within different types of Shariah contracts used to structure financial products. A robust and dynamic

risk assessment approach is required for products that involve different types of Shariah contracts throughout the life of the product.

27. While risk measurement models are important components of risk management, the use of risk modelling and quantitative risk methodologies should be tempered with expert judgement and critical analysis by senior management and reviewed by the board. Financial institutions should avoid excessive reliance on such models. The board and senior management should be well informed of the underlying assumptions, potential limitations and uncertainties relating to the output of the risk models and systems which could impair the accuracy of risk estimates. Similarly, external assessments (e.g. ratings by external rating agencies) should only be used as inputs to internal risk assessment processes and should not form the sole basis for risk-taking decisions. The financial institution remains ultimately responsible for assessing risk and should therefore view external risk assessments critically and maintain adequate internal processes to evaluate the appropriateness of their use by the institution.

28. The use of models for identifying and measuring risk should be supported by robust processes for managing model risk. This should include effective oversight by senior management of model development and implementation, establishing limits on model use, monitoring model performance, and regular and independent model validation.

29. Financial institutions must ensure that its risk management framework is responsive to changes in or expansion of business activities, and developments in the operating environment. The framework should support the ability of financial institutions to anticipate and react quickly to new or emerging risks. Financial institutions should perform stress tests which capture material sources of risk and adopt plausible adverse scenarios, as part of their risk management process and integrate the results of the stress tests into its decision making[5]. In addition, financial institutions should also regularly review actual performance

[5] This principle should be read together with the Guidelines on Stress Testing issued by the Bank.

after the fact relative to risk estimates (i.e. backtesting) to gauge the appropriateness and effectiveness of risk management policies, processes and methodologies.

30. To support the ability to make informed and timely risk decisions, financial institutions must have in place information systems that provide current, complete and accurate information on the size, quality and composition of exposures across risk types and material products and counterparties to all relevant levels in the financial institution[6]. The sophistication of the financial institution's information systems must keep pace with developments in the institution's risk profile, increasing business complexity, and new product or business lines. For larger and more complex financial institutions, greater attention must be given to ensuring that data can be consolidated quickly to provide an enterprise-wide view of risks.

31. When developing strategies or responses to mitigate risks, consideration should be given to the impact of the chosen mitigation strategy on other risks, directly or indirectly. These should be explicitly considered and accounted for, to avoid giving rise to new unattended risks. The board should periodically review the effectiveness of risk mitigation strategies post implementation.

32. Appropriate governance processes must be established for new business or risk-taking activities, such as new products or material modification to existing products, new lines of business or entry into new markets, as well as expansions through mergers and acquisitions, to ensure that risks have been properly assessed and that the institution's risk management systems are able to accommodate and support such activity.

33. The risk management framework must address end-to-end risks in the product life cycle in a manner consistent with expectations set out under the Bank's

[6] This principle should be read together with the Guidelines on Data Management and MIS Framework issued by the Bank.

Guidelines on Introduction of New Products and Guidelines on Introduction of New Products for Insurance Companies and Takaful Operators. This includes, amongst others, ensuring that staff in the marketing/distribution and advisory function for financial products have an adequate understanding of risks and have access to appropriate training to support their roles in contributing to risk outcomes for the financial institution.

34. The risk management framework and culture should impose expectations on business lines and other functions to also support the risk management function. Relevant staff in the business lines and other functions should be encouraged to be aware of changes in the market environment and its influence on risk, and to recognise and report when conditions or assumptions change such that assessments can be updated.

Principle 5: Risk management must be well-integrated throughout the organisation and embedded into the culture and business operations of the institution.

35. The board and senior management must ensure that risk management activity is not carried out in isolation but is well-integrated throughout the organisation. Financial institutions must promote the awareness and understanding of risks throughout the institution and ensure that risk management is embedded into their business practices so as to enable employees to take into account risks and its impact to the financial institution in their business decision-making. This may include formal processes for authorisation from independent risk management function for key business decisions.

36. The organisational structure, processes and information flows for managing risk must promote an organisation-wide awareness of risk and integrated management of risk across risk categories (e.g. credit, market, operational, liquidity), across products and business lines, as well as at the institution and group-wide level. Financial institutions must be able to demonstrate how risk correlations and risk concentrations within and across the various business units

in the institution or the group have been accounted for under an integrated risk management approach so that the board and senior management have an overview of the magnitude of aggregate risks affecting the organisation. This should serve to ensure that the risk-taking activities remain consistent with the overall risk appetite approved by the board.

Principle 6: Financial institutions must establish an independent senior risk executive role (chief risk officer or its equivalent) with distinct responsibility for the risk management function and the institution's risk management framework across the entire organisation. The executive must have sufficient stature, authority and seniority within the organisation to meaningfully participate in and be able to influence decisions that affect the financial institution's exposures to risk.

37. The role of the chief risk officer (CRO) must be distinct from other executive functions and business line responsibilities. Institutions must not combine the CRO role with other executive functions ("dual hatting" i.e. where the chief operating officer, chief financial officer or other senior management also serves as the CRO). In addition, the CRO must not have any management or financial responsibility in respect of any business lines or revenue-generating functions.

38. Smaller and less complex institutions may combine the CRO with another control function (other than internal audit[7]). In such cases, the board must be satisfied that a sound overall control environment will not be compromised by the combination of responsibilities for key control functions in a single individual.

39. The reporting lines must be established to appropriately reflect the importance of the role and accountability of the CRO. Hence, the CRO must be positioned at a sufficiently senior level in the organisation to enable risk considerations to be raised directly to the board and senior management and duly taken into account

[7] The CRO must not be primarily responsible for internal audit as this would render the independent review process ineffective.

in management decisions. The CRO in turn, must ensure that the risk management function is credible and effective and that its views and recommendations on risk matters receive the appropriate attention from the board, senior management and business lines.

40. To preserve the CRO's independence, the CRO must report and have direct and unimpeded access to the board and its risk committee. In addition, the appointment, remuneration and dismissal of the CRO must be subject to the approval of the board or the board-risk committee. For cases of resignation of the CRO, the board must have in place an internal process to understand the reasons and circumstances leading to the resignation.

41. The position of the CRO within the institution should also allow for regular and timely communication with the CEO and senior management to ensure that they are kept informed of and engaged in material risk developments that would be critical to their functions and primary responsibilities.

42. The CRO must have good knowledge of the business and the relevant qualifications, technical skills and experience in risk disciplines to enable him to lead the effective implementation of the risk management framework for the financial institution. The CRO should also have strong communication skills to be able to effectively engage the board on risk matters and constructively interact with the CEO and other senior management on risks affecting the financial institution.

Principle 7: Financial institutions must establish and maintain an effective risk management function with sufficient authority, stature, independence, resources and access to the board.

43. The risk management function is responsible for identifying, measuring, monitoring, controlling and reporting on the institution's overall risk exposures.

This should encompass risks at firm-wide, group-wide, portfolio and business-line level, as well as both on- and off-balance sheet exposures.

44. The risk management function should be involved in the business planning process so as to ensure that the institution's growth strategy is compatible with the institution's risk appetite with adequate and independent consideration of potential risks. It should also be able to contribute risk perspectives to business decisions to ensure the alignment of business and risk strategies.

45. The risk management function must be independent of the business units whose activities and exposures it reviews. At the same time, it should have an in-depth understanding of the activities and their implications to the risk profile of the institution and access to those business units. The internal relationships of the risk management function with business lines and senior management should be properly defined and actively monitored to ensure that the risk management function remains effective and independent of business and operational decisions.

46. The risk management function must be equipped with risk management personnel who possess sufficient experience and qualifications, including market and product knowledge as well as sound and practical knowledge of risk disciplines to enable them to provide specialised analysis and perform effective risk reviews. The level of expert knowledge and experience should be commensurate with the institution's risk profile.

47. Risk management personnel should have the ability, credibility and willingness to challenge business lines regarding all aspects of risk arising from the institution's activities.

48. The risk management function must also be equipped with adequate resources and support (including IT support) to perform its roles. It must additionally be given full access to internal systems and information for the purpose of performing its roles.

49. For insurance companies, the risk management function must be appropriately supported by actuarial expertise to assess the insurer's actuarial and financial risks. Consistent with paragraph 45, actuarial expertise supporting the risk management function must not also be directly responsible for, or have a major role in directing business decisions, including product development and design, investment strategies and pricing policies[8].

Principle 8: Effective implementation of the risk management framework must be reinforced with an effective compliance function and subjected to an independent internal audit review.

50. The compliance function must form part of the institution's risk management control functions and contribute to the determination of compliance risk measurement and assessment, and the development of appropriate procedures for controlling identified compliance risks.

51. The compliance function is responsible for ensuring the financial institution's compliance to the applicable laws, regulations, internal policies, procedures, and limits (including risk limits). Its key responsibilities should include maintaining policies and procedures to detect and minimise risk of non-compliances and to assess the adequacy and effectiveness of such policies and procedures on an on-going basis.

52. The compliance function should interact closely with the risk management function to bring risk issues to the attention of risk management and cooperate in developing mitigation measures. Additionally, the compliance function should also cooperate with other functions (e.g. legal, finance) to promote effective controls in managing compliance risk.

[8] Insurance companies or takaful operators which require additional time to meet the requirement described under paragraph 49 may submit relevant plans and timelines for achieving compliance to this requirement as provided under paragraph 76.

53. The risk management framework must be subjected to an in-depth review by the internal audit function[9] which performs a key role in providing assurance to the board that the financial institution is operating in a sound control environment and ensuring that control weaknesses are appropriately dealt with. The internal audit function must report regularly to the board and senior management on the effectiveness and adequacy of the risk management and compliance functions, and whether the internal controls in the organisation are working effectively. The board must ensure that internal audit staff have skills and competencies that are commensurate with the business activities and risk profile of the institution to effectively perform their roles.

54. Appropriate structures and lines of reporting between the compliance, internal audit and risk management function must be clearly defined to ensure the timely communication of issues which have an impact on the effectiveness of the institution's risk management framework and their prompt escalation to the board and senior management.

55. The board and senior management should also support initiatives that are directed at improving and contributing to the effectiveness of these functions. This shall include allocating sufficient resources to these functions and ensuring that these functions are continuously strengthened to cope with expansions in risk-taking activities and more challenging business environment.

Principle 9: Financial institutions must have appropriate mechanisms in place for communicating risks across the organisation and for reporting risk developments to the board and senior management.

56. Board and senior management must be equipped with timely, complete, meaningful and accurate risk information to enable them to make informed

[9] This paragraph should be read in conjunction with the Guidelines on Corporate Governance for Licensed Institutions and the Guidelines on Internal Audit Function of Licensed Institutions issued by the Bank, which provide further expectations on the role of internal audit.

decisions. The board or its risk committee must establish the frequency, content and form of risk reports to be submitted to the board so as to ensure the risk reports facilitate understanding and the determination of appropriate risk responses. The board must also institute periodic reviews of the amount, form and quality of risk information that the board receives.

57. Information provided to the board and senior management should present an accurate, complete and "unfiltered" (i.e. does not suppress negative information) view of material risks in a way that supports informed decisions. The board should be aware that excessive detail, volume and complexity in the content of the risk reports can lead the board to overlook critical risk developments and complicate an accurate picture of the institution's overall key risk exposures. The board and senior management must have high-level risk information and the ability to drill down into specific risk areas where more detailed information can be made available, which will assist the board in providing constructive challenge to senior management.

58. Financial institutions must establish risk monitoring and reporting requirements across the organisation. These should include the development and use of key risk indicators to provide early warnings on adverse risk developments to ensure institutions are able to manage and mitigate their risks in a timely manner.

59. Risk monitoring and reporting should be performed at the business unit and portfolio level, as well at the firm-wide and group-wide level. Deficiencies or limitations of risk estimates as well as any significant embedded assumptions must be clearly communicated. Risk reporting systems should also be dynamic, comprehensive and accurate, and draw on a range of risk analytical tools and approaches and should be subject to independent periodic reviews by the risk management function and internal audit.

VI. Remuneration

Principle 10: Executive remuneration must be aligned with prudent risk-taking and appropriately adjusted for risks. The board must actively oversee the institution's remuneration structure and its implementation, and must monitor and review the remuneration structure to ensure that it operates as intended.

60. The board must be satisfied that the overall remuneration policy does not induce excessive risk-taking and is consistent with the risk appetite and the long-term strategy of the financial institution.

61. Remuneration structures[10] must reinforce prudent risk-taking and be appropriately adjusted for risks. Performance metrics used in determining remuneration must not contribute to the misalignment of risk and reward. Performance goals or expectations imposed on employees (other than in control functions) should appropriately balance between achieving business outcomes and engendering responsible risk behaviours.

62. Remuneration structures should reflect the nature and time horizon of risks. Since the time horizon of performance and associated risks can vary, financial institutions should consider a multi-year framework in the measurement of performance. The board must also consider an appropriate mix of fixed and variable components (i.e. the mix of cash, equity and other forms of remuneration) and how components of remuneration may impact risk-taking behaviours and contribute to or undermine the institution's risk management objectives.

63. Board members who are tasked to review the design and operation of the remuneration system must be independent, non-executive members, and must collectively have an adequate understanding of the institution's risk profile,

[10] This should also include incentive structures offered to insurance and takaful agents.

including its risk drivers and risk measurement and management capabilities, and of how different remuneration practices can impact the institution's risk profile.

64. The board should ensure that persons performing control functions have input in setting remuneration policies for other business areas to promote the alignment of risks and rewards across the organisation.

65. Remuneration for employees in control functions must be structured in a way that is principally based on the achievement of their control objectives and does not compromise their independence.

66. Due care should be exercised to preserve a clear distinction between performance measures of staff responsible for control functions and the performance of any business unit. Where risk and compliance functions are embedded in the business units, a clear distinction must be made between the remuneration policy applicable to staff undertaking the control functions and other staff in the business unit.

67. The board or its risk committee must be actively involved in the performance reviews of individuals primarily responsible for control functions.

VII. Complex and opaque corporate structures

Principle 11: The board and senior management must be aware of and understand the financial institution's operational and organisational[11] structure and the risks it poses and be satisfied that it is not overly complex or opaque such that it hampers effective risk management by the financial institution.

68. The creation of structures in the form of units, branches, subsidiaries or other legal entities to achieve legal, regulatory, or funding needs or for product-offering purposes can increase the complexity of the organisation due to the sheer number of related entities and level of interconnectedness as well as the intra-group transactions. The board and senior management must consider how risks associated with the institution's operational and organisational structures affects its ability to manage risks on an enterprise-wide and group-wide basis and the implications for capital and funding strategies. This requires a sound understanding of the operational and organisational structure of the financial institution and the group including the business focus of the various entities within the group, the relationships among them and the nature and extent of intra-group exposures. Such information should be properly documented and regularly updated as an integral part of the financial institution's risk management process. Additionally, effective measures and systems must be in place to facilitate the generation and exchange of information among the various entities, so as to facilitate the assessment and management of risks faced by the financial institution and the group as a whole.

69. For larger and more complex organisations, the effectiveness of the parent company's board oversight over the entire group can be enhanced by requiring a control function to conduct a formal review of the structures, controls and

[11] Organisational structure refers to the formal structure of entities within a corporate group. Operational structure may differ from the organisational structure such as in instances where certain business or control functions are centralised within a corporate group.

activities within the group. This review should seek to assess whether the organisation of existing structures, controls and activities are contributing to the overall efficiency and effective control of the group or increasing risks to the financial institution. It should also determine if the policies, controls and activities of the group are consistent with the board-approved risk strategies both for the financial institution and the group as a whole. The board and senior management should be informed of the findings of the review.

Principle 12: Where a financial institution operates through special-purpose structures, its board and senior management must understand the purpose, structure and unique risks of these operations. Appropriate measures must be undertaken to mitigate the risks identified.

70. Financial institutions must consider the extent to which operating through structures that are not fully transparent poses financial, legal, reputational or other risks to the financial institution, or impedes the ability of the board and senior management to conduct appropriate risk oversight.

71. The board and senior management should evaluate the proposed activities of special-purpose structures and carefully consider, prior to operating such structures, how effective and appropriate risk oversight can be instituted over these structures. Activities carried out through special purpose structures must be subject to regular internal audit reviews.

72. The board and senior management must periodically monitor such structures and activities to ensure that they remain consistent with their established purposes. In addition, there must be supporting controls and processes to ensure that structures and arrangements that support regulatory capital relief meet the relevant operational requirements and conditions on legal certainty on a continuing basis.

VIII. Role of subsidiary and parent entities with respect to risk governance

Principle 13: The board and management of subsidiary financial institutions will be held responsible for effective risk management processes at the subsidiary level and must have appropriate influence in the design and implementation of risk management in the subsidiary. Conversely, the board and management of a parent financial institution with local and overseas operations is responsible for the risk management of the group and must exercise oversight over its subsidiaries with appropriate processes established to monitor the subsidiaries' compliance to the group's risk management policies.

73. The Bank recognises that locally incorporated subsidiary of foreign financial institutions are subject to group practices in respect of risk management strategies and may leverage on the group's risk management systems and capabilities. Notwithstanding these practices, the local subsidiary board remains responsible for and will be expected to observe the risk governance principles contained in this policy in relation to the subsidiary. In particular, the local subsidiary board must ensure the suitability of the group approaches and methodologies adopted, having regard to the context of the local environment and operations of the subsidiary.

74. From the perspective of a locally incorporated financial institution with local and overseas operations, the board of the parent company must be responsible for overseeing strategic, group-wide risk assessments and management, and approving group-wide corporate risk policies. In doing so, the board must:

    i. be aware of the material risks and issues in the subsidiary that might affect the financial institution or group;
    ii. ensure that the subsidiaries' reporting obligations to the head office have been established; and

iii. ensure that reporting obligations of the subsidiaries have been clearly communicated, and are effectively complied with, to support group-wide assessment of and responses to risk developments.

75. Financial institutions should ensure that appropriate monitoring processes of other material investments such as joint ventures and associates, have been established to enable timely identification and management of risks, including reputational risk, stemming from these entities.

PART C IMPLEMENTATION

IX. Implementation Requirements

76. This policy is effective from 1 March 2013. Financial institutions, upon application to the Bank, may be given additional time to bring existing practices and policies in line with the principles set out in this policy document. Such institutions must be able to identify non-compliant practices and demonstrate concrete plans of action with specific timelines for achieving full observance of the principles.