ANNEX 1

GUIDELINES

ON

RISK MANAGEMENT FRAMEWORK

Date: 27 December 2018

CONTENTS

I. BACKGROUND

A. Introduction

1. There are numerous definitions of risk. For the purposes of these Guidelines, risk is defined as negative outcomes in the form of financial losses incurred by a bank or banking group arising from future outcomes and impacting its financial performance and financial position.

2. It is imperative for a bank proactively to manage its risk profile. Through the discipline of risk management, a bank or banking group can materially improve its future outcomes and thereby dampen negative impacts and strengthen positive impacts. A bank's risk appetite must enable it to strike a prudent balance between the level of risk it is willing to expose itself to (its desired risk profile) and the level of return it seeks to generate (its desired return on capital), thereby ensuring its financial survival and sustainability. In summary, a bank must have an effective risk management framework that is commensurate with the nature and extent of its strategic plan, business operations, its financial position, financial performance and financial resources.

3. A bank must establish a sound and effective system to manage its risks, including credit risk, market risk, interest rate risk / profit rate risk, liquidity risk, operational risk, reputation risk, legal risk and strategic risk. A bank is also required to have adequate internal systems for assessing capital adequacy in relation to the risks it assumes. According to the Basel Committee on Banking Supervision pronouncement titled Core Principles for Effective Banking Supervision, dated 2012, a bank must have in place a comprehensive risk management process (including board and senior management oversight) to identify, measure, evaluate, monitor, report and control or mitigate all material risks on a timely basis and to assess the adequacy of their capital and liquidity in relation to their risk profile and market and macroeconomic conditions. The risk management process must be commensurate with the risk profile and systemic importance of the bank.

B. Application

4. These Guidelines set out AMBD's expectations regarding a bank's risk management framework. These Guidelines must be read with other relevant Guidelines[1] and the pronouncements of the Basel Committee on Banking Supervision.

5. For the purposes hereof, risk (management) framework means, collectively, the governance, systems, structures, policies, procedures and people that identify, measure and evaluate, control and mitigate, monitor, and report risk on a bank-wide (and group-wide) basis.

6. AMBD will apply these Guidelines to banks on a proportionate basis, having regard to their size, nature and complexity of operations. Thus, a bank having a relatively small and simple business operation may not need to adopt and operate a risk management framework which is as extensive and as sophisticated as that of a large complex bank. In general, a bank must apply these Guidelines both on a solo-entity basis and, where applicable, a consolidated basis, covering, where applicable, its subsidiaries, associated companies and joint ventures, with particular focus on potential sources of significant risk.[2]

[1] Such as Guidelines on Corporate Governance, Credit Risk Management, Internal Audit Function, Compliance and Compliance Function, Internal Control Systems etc.

[2] Whether the standards must be applied to associated companies or joint ventures will also depend on the extent of a bank's affiliation to the entities and the level of control it can exercise over the entities.

7. International banking groups operating in Brunei must have a three lines of defence framework, including a risk management framework, appropriate for their local operations. Where certain risk management functions pertaining to a banking group's local operations are centralised at the bank, regional or group level, the bank must be able to demonstrate that the relevant functions performed at the bank, regional or group level are appropriate for the size, nature and complexity of the local operations and are in line with the standards in this Guideline.

8. A bank wishing to be considered for the application of a proportionate approach must submit a written motivation for the AMBD's consideration. The motivation must describe and explain how the proportionate approach will enable the bank to discharge its responsibilities. Permission to apply a proportionate approach will be subject to the bank performing annual and ad hoc reviews (when circumstances dictate the need for ad hoc reviews) as well as commissioning triennial independent reviews. The bank must submit such a review to the AMBD within one month of completion thereof.

9. Failure to adhere to these Guidelines may call into question whether a bank continues to satisfy the minimum criteria for bank licensing and cast doubt on the fitness and propriety of the bank's directors and senior management.

10. The risk (management) framework must clearly: -

a. Identify the governance structures used to manage risk, including reporting lines and accountabilities;

b. Describe the bank's approved risk appetite;

c. Describe the risk measurement and assessment tools and how they are used;

d. Specify standards for valuing exposures and measuring performance;

e. Detail thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

f. Establish and maintain risk reporting and management information systems for comprehensive risk reporting;

g. Describe effective internal controls, including compliance and independent assurance;

h. Provide for a common taxonomy of risk terms to ensure consistency of risk identification exposure rating and risk management objectives;

i. Provide for appropriate independent review and assessment of risks; and

j. Require policies to be reviewed whenever a material change in the risk profile of the bank occurs and revised as appropriate.

II. KEY ELEMENTS

A. Risk (management) governance framework

11. Risk governance refers to the formal arrangements that enable the board of directors (board) and senior management of a bank to develop and adopt a risk management framework, establish a business strategy, articulate and monitor adherence to risk appetite and risk limits, and identify, measure and assess, mitigate and control, monitor, and report risks.

12. A bank's risk (management) governance framework must be aligned with the specific circumstances of the bank, particularly its risk profile, scale, nature, business focus and mix, complexity and systemic importance.

13. To ensure effective risk management, a bank must have in place a set of robust risk governance arrangements, whereby responsibilities of the board and senior management, and other distinct functions of the bank (and the respective risk owners), are well-defined. The risk governance framework must also outline escalation and notification procedures (including to the board and senior management) as well as potential disciplinary actions for compliance breaches and excessive risk-taking by individuals.

14. Risk management, compliance and internal audit comprise key control functions in a bank. The control functions have a responsibility, independent of the management of a bank's business lines, to provide objective assessment, reporting and/or assurance, thereby making an indispensable contribution to effective corporate governance.

15. The dispersion of responsibilities among the distinct functions of the bank must be organised to give effect to three lines of defence which are independent from each other: -

a. the first line of defense is provided by the business units where risks are taken in pursuit of revenue generation and all supporting functions.[3] Business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable. When conducting business activities, staff in the business units hold frontline positions in the proper identification, measurement, assessment, mitigation and controlling, monitoring, and reporting of risk exposures on an ongoing basis, having regard to the bank's risk appetite, and policies, procedures and controls. The roles and responsibilities of risk owners in business units must be clearly defined.[4]

b. the second line of defense is provided by independent risk management and compliance functions. The risk management function is primarily responsible for overseeing the bank's risk-taking activities, undertaking risk assessments and reporting independently from the business line, while the compliance function monitors compliance with laws, corporate governance rules, regulations and internal policies; and

[3] A more expansive definition of the first line of defence includes all functions other than second and third lines of defence.

[4] For instance, the person heading a business unit, as a risk owner must ensure that activities of the unit are in line with the bank's approved risk appetite, approved risk limits are adhered to, necessary internal controls and risk management processes (particularly those relating to the identification, monitoring and reporting of the use of allocated risk limits) are effectively implemented, and any breaches of risk limits and material risk exposures are promptly reported to the chief risk officer and the senior management.

c. the third line of defence is provided by an independent and effective internal audit function, which is responsible for providing assurance on the effectiveness of the bank's risk management framework, including the risk governance arrangements (including the first and second lines of defence described above).

16. Risk governance arrangements must be documented and updated as appropriate. A bank must have appropriate procedures in place to ensure that all relevant staff (including business units) are aware of and understand these arrangements and their respective roles in the oversight and management of risk.

17. An overview of how these elements fit together is illustrated in **Attachment A**. This illustration is not intended to be prescriptive.

18. Senior management is responsible for developing, for board approval, a clear effective and robust risk management governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for presenting the risk management governance structure to the board of directors for approval, implementing the approved risk governance structures, and periodically reviewing it.

19. Regarding a committee structure: -

a. Sound industry practice for larger and more complex organisations with a central group risk management function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level risk type committee reports.

b. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from risk type committees by country, business or functional area.

c. Smaller or less complex organisations may utilise a flatter organisational structure which oversees risk type directly with the board's risk management committee.

20. Regarding a committee composition: -

a. Sound industry practice is for risk type committees to include a combination of members with expertise in business activities and financial, as well as independent risk management.

b. Committee membership can also include independent non-executive board members, which is a requirement in some jurisdictions.

21. Regarding committee operation: -

a. Committee meetings must be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making.

b. Records of committee operations must be adequate to permit review and evaluation of committee effectiveness.

B. Risk (management) culture

22. Effective risk governance requires a strong risk culture[5] which promotes risk awareness and encourages open communication and challenge regarding risk-taking across the bank (including vertically to and from the board and senior management). Obstacles that impede legitimate sharing of information across distinct functions within a bank (e.g. competition between, or incompatible IT systems among, business lines) must be avoided, as such obstacles may result in decisions being made in silos which may not be in the best interest of the bank,[6] while complying with privacy and confidentiality prescriptions.

23. Information communicated to the board and senior management must be timely, accurate and presented in an understandable and concise format. Material risk-related information that requires immediate decision or reaction must be promptly presented to senior management and the board (as appropriate), the responsible officers and, where applicable, the heads of control functions, so that suitable measures can be initiated at an early stage.

24. The board of directors is responsible for taking the lead in establishing and maintaining a strong risk management culture throughout the whole organisation. The board of directors and senior management must establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behavior.

25. Banks that have a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur.

C. Risk appetite framework

26. The development of the risk appetite framework of a bank must be driven by leadership from the board and senior management, supplemented as appropriate by the involvement of management at functional and affiliated entity levels. A bank's risk profile must be aligned to the bank's risk appetite.

27. The establishment, implementation and ongoing review of a risk appetite statement and risk limits are key to a sound risk appetite framework. The risk governance framework must facilitate the embedding of the risk appetite into the bank's risk culture through communication, monitoring and reporting.

[5] Risk culture refers to a bank's norms, attitudes and behaviors related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. A bank's risk culture influences the decisions of senior management and staff during their day-to-day activities and has an impact on the risks they assume.

[6] For the avoidance of doubt, nothing in this paragraph is intended to affect a bank's obligations to comply with any Chinese Wall or other legal requirement mandating the maintenance of data confidentiality.

III. RESPONSIBILITIES OF BOARD AND SENIOR MANAGEMENT

A. Overall responsibilities

28. The board of directors of a bank is in ultimate and overall control of the bank and, consequently, bear the ultimate responsibility and accountability for oversight over the bank's risk management framework. The board of directors delegate the day-to-day management responsibility for the risk management framework to the senior management.

29. The board and senior management of a bank have the primary responsibility to understand the overall risk profile of a bank and ensure that the risks run by the bank are properly managed. In particular, the board and senior management must have a clear vision of the significant risks faced by the bank.

30. In fulfilling this responsibility, the board and senior management must, among other things:

a. have sufficient knowledge and expertise to understand all material risks faced by the bank, including the risks associated with new or complex products and high-risk activities, and the interaction of these risks under stressed conditions;

b. Have direct involvement in setting, and monitoring adherence to, the bank's risk appetite, which must be commensurate with its operations and strategic goals;

c. create a strong risk culture throughout the bank and ensure that the bank's risk appetite is well-enshrined within the culture;

d. establish an organisation and management structure with a sound control environment, adequate segregation of duties and clear accountability and lines of authority;

e. dedicate sufficient time, effort and resources to overseeing and participating in the bank's risk management process, with a full and ongoing commitment to risk control;

f. evaluate regularly the risks faced by the bank, and maintain continued awareness of the bank's business and risk profiles and changes in the operating environment and financial markets that may give rise to emerging risks;

g. ensure that the necessary infrastructure, systems and controls are developed and maintained to support effective risk management and governance;

h. set up effective controls to ensure the integrity of the bank's overall risk management process and to monitor the bank's compliance with all applicable laws, regulations, supervisory standards, best practices and internal policies and guidelines;

i. ensure that the bank's remuneration systems are consistent with, and promote, effective risk management and do not incentivise imprudent or excessive risk-taking; and

j. promote the establishment of regular and transparent communication mechanisms within the organisation.

B. Setting of risk appetite and monitoring

31. The board must develop in collaboration with senior management and approve a bank risk appetite framework and ensure that it is consistent with the bank's strategic, business, capital and financial plans, as well as the bank's risk-taking capacity and remuneration system.

32. The board is responsible for setting the bank's overall risk appetite and approving the risk appetite statement recommended by the senior management. While there is no standard means of expressing a bank's risk appetite, it must be articulated clearly and concisely to facilitate internal communication and implementation. The level of detail and sophistication of a bank's risk appetite statement must be commensurate with the bank's business nature and risk management needs. A bank's risk appetite statement must as far as practical: -

a. express the bank's overall risk appetite in a manner that is suitable for the nature and complexity of its business, with all relevant risks taken into account, including those arising from off-balance sheet transactions and risks that are less quantifiable (e.g. reputation risk). This may involve assessing both the financial and non-financial implications of risks, through quantitative analysis, stress-testing, reference to historical experience, exercise of judgement or otherwise;

b. set out the maximum level of each material risk and of the overall risks that the bank is prepared to take in pursuit of its strategic and business plans, having regard to the applicable regulatory and legal requirements;

c. address quantifiable risks with quantitative measures that can be translated into risk limits applicable to business units (at individual entities and group level) which in turn can be aggregated and disaggregated to enable measurement of the bank's risk profile against its risk appetite and risk-taking capacity;

d. include qualitative statements that articulate clearly and concisely the motivations for taking on or avoiding certain types of risks which are less quantifiable in nature (e.g. legal risk, reputation risk and conduct risk), and establish some indicators to enable monitoring of such risks;

e. include key background information and assumptions underlying the established risk appetite, which may, as appropriate, define the boundaries and considerations for the formulation of the bank's strategic and business plans; and

f. be forward-looking and include appropriate financial targets that are consistent with the bank's risk appetite and outline possible measures and actionable elements that reflect the bank's intended responses to a range of possible events, e.g. a loss of capital or a breach in risk limits. Possible management actions outlined in the statement must be realistic and feasible for restoring capital or reducing risk in adverse situations and must not be inconsistent with the bank's recovery plan (where applicable).

33. The board must be satisfied that, and should periodically assess, the extent to which, the senior management has put in place robust procedures and controls for implementing and monitoring adherence to the bank's risk appetite framework and its risk appetite statement. Sufficient information must be compiled to facilitate regular assessment by the board and senior management of the management of risk against the bank's risk appetite, such as: -

a. relevant measures of risk (e.g. based on economic capital or stress tests);

b. a view of how risk levels compare with limits;

c. the level of capital that the bank would need to maintain after sustaining a loss of the magnitude of the risk measure; and

d. the actions that management could take to restore capital after sustaining a loss.

34. The risk appetite statement must be used as the basis for the board, senior management, business units and internal control functions to deliberate upon and formulate the bank's strategic, business, capital and financial plans. Strong direction from, and the engagement of, the board is critical to sustaining a disciplined risk appetite for the bank. When faced with, and making decisions in response to, new business opportunities (e.g. possible business expansion or mergers and acquisitions), market demand for increased risk-taking or the need to react promptly to changes in the external environment (e.g. due to competition or deterioration in economic conditions), the board must ensure that there is an assessment of the bank's risk appetite in the decision-making process. In these circumstances, the bank must thoroughly understand the bank's current risk position relative to its risk appetite, and how that position would be changed if the risk appetite were to be changed. In this regard, stress tests may be used to generate a dynamic view of the bank's capital, liquidity and risk positions.

35. Any changes to the bank's risk appetite statement must be approved by the board. The justification for change must be adequately documented.

C. Firm-wide risk management

36. The board and senior management must ensure that effective policies, processes and systems are in place to identify, measure, evaluate, monitor, report and control or mitigate all material risks across business activities, whatever the nature of the exposure arising from those activities (such exposure may be non-contractual, contingent or off-balance sheet in nature).

Specific responsibilities of the board

37. To ensure adequate oversight of risk-wide risks, the board must, among other things, be responsible for: -

a. approving a firm-wide definition for distinct types of risk faced by the bank (for risk appetite statement and other purposes);

b. identifying, understanding and assessing the risks inherent in the bank's business activities or in new products or services to be launched;

c. laying down risk management strategies and approving a risk management framework developed by senior management based on these strategies which is consistent with the bank's business goals and risk appetite;

d. determining that the risk management framework is properly implemented and maintained by senior management;

e. reviewing the risk management framework periodically to ensure that it remains adequate and appropriate under changing business and market conditions;

f. ensuring that independent risk management and control functions are robust, truly independent from the bank's risk-taking functions (both in terms of decision-making and reporting structure), and have sufficient authority, resources, expertise and competence to carry out their functions.

Specific responsibilities of senior management

38. Senior management must be responsible for: -

a. formulating detailed policies, procedures and limits for managing different aspects of risk arising from the bank's business activities, based on the risk management strategies laid down by the board.

b. designing and implementing a risk management framework to be approved by the board and ensuring that the relevant control system within the framework work as intended. The framework must be implemented throughout the whole organisation with appropriate procedures to ensure that all levels of staff are aware of, and understand, their responsibilities with respect to risk management;

c. putting in place processes for reviewing the bank's risk exposures and ensuring that they are kept within the risk limits set, and that those limits are consistent with the bank's overall risk appetite, even under stressed conditions;

d. identifying and acting on emerging risks and, where appropriate, reporting any material risks to the board promptly; and

e. ensuring the competence of managers and staff responsible for risk management and control functions, with appropriate programs to recruit, train and retain employees with suitable skills and expertise.

D. Use of specialised committees

39. While the board is ultimately responsible for risk management, it may be beneficial for it to delegate authority to appropriate board-level committees to carry out some of the risk management tasks described above ***(see paragraph 37 above)***. Delegation of authority must be made on a formal basis with a clear mandate.

40. It must be clearly recognised, however, that such delegation of authority does not absolve the board and its members from their risk management responsibilities and the need to oversee the work of the specialised committee(s) exercising delegated authority. Individual board members are expected to have an adequate understanding of the nature of the bank's business activities and the associated risks as well as the framework, including the major controls (e.g. risk limits used to manage the risks.[7] If existing members lack the relevant expertise, bringing in new members with such knowledge or appointing external consultants must be considered.

[7] For example, some members must preferably have practical experience in financial markets and risk management or have obtained, from their business activities, sufficient professional experience directly linked to such type of activity.

41. All locally incorporated banks must establish a risk committee. All other banks are strongly encouraged to do so. The risk committee must: -

a. be a stand-alone committee and distinct from the board audit committee;

b. be chaired by an independent non-executive director with a background in accounting, banking or other relevant financial industry, or expertise in risk management. “Dual-hatting” with the chair of the board or any other committee must be avoided;

c. be composed of a majority of members who are independent non-executive directors. Members of the risk committee must collectively possess relevant technical expertise and experience in risk disciplines that are adequate to enable them to discharge their responsibilities effectively;

d. review and recommend for the board’s approval the bank’s risk management strategies, key risk policies and risk appetite, at least annually;

e. exercise its authority (if delegated by the board) to review and approve specified types of risk management policies and procedures, as appropriate;

f. review and assess the adequacy of the bank’s risk management framework and policies in identifying, measuring, monitoring and controlling risks and the extent to which these are operating effectively;

g. oversee the establishment and maintenance by senior management of appropriate infrastructure, resources and system for risk management, particularly in relation to the bank’s adherence to the approved risk appetite and related policies;

h. oversee and discuss the strategies for capital and liquidity management, and those for all relevant risks (on both an aggregated basis and by type of risk) of the bank, to ensure they are consistent with the stated risk appetite;

i. oversee and challenge the design and execution of stress testing and scenario analyses;

j. review periodic reports provided by the senior management (including the chief risk officer) on the state of the bank’s risk culture, risk exposure and risk management activities;

k. ensure that the staff members of the bank responsible for implementing risk management systems and controls are sufficiently independent of the bank’s relevant risk-taking activities; and

l. examine, without prejudice to the tasks of the remuneration committee, whether incentives created by the remuneration system are aligned with the bank’s risk culture and risk appetite, and whether remuneration awards appropriately reflect risk-taking and risk outcomes.

IV. RISK MANAGEMENT POLICIES, PROCEDURES AND LIMITS

A. Policies and procedures

42. Banks must have clearly defined and documented policies and procedures that enable firm-wide risks to be managed in a proactive manner,[8] with emphasis on achieving: -

a. objective and consistent risk identification and measurement approaches;

b. comprehensive and rigorous risk assessment and reporting systems;

c. sound valuation and stress-testing practices; and

d. effective risk monitoring measures and controls.

43. Risk management policies and key risk management procedures must be approved by the board (or its designated committee(s) with the necessary delegated authority). Detailed operating procedures can be approved by the management at the appropriate level.

44. The risk management policies and procedures must be developed based on a comprehensive review of all business activities of a bank, and cover all material risks, both financial and non-financial (e.g. reputation risk) associated with the bank's activities. They must be prepared on a firm-wide basis and, where applicable, on a group-wide basis.

45. The development of risk management policies and procedures must take account of the following factors: -

a. a bank's overall business strategy and activities;

b. the appropriateness to the size, nature and complexity of the bank's business activities;

c. the risk appetite of the bank;

d. the level of sophistication of the bank's risk monitoring capability, risk management systems and processes;

e. the bank's past experience and performance;

f. the economic substance of the bank's risk exposures (including reputation risk and valuation uncertainty);

g. the results of sensitivity analysis and stress tests;

h. anticipated internal or external changes (e.g. planned operational changes or expected changes in market conditions); and

i. any legal and regulatory requirements.

[8] A registered foreign bank branch may, to a large extent, apply the firm-wide policies and procedures set by its head office to their local operations, provided that such documents are customised to take account of local market conditions.

46. Accountability and the lines of authority for each business line or unit (including the head and any other relevant principal officers of such business line or unit) must be spelled out clearly in the policies and procedures and updated as appropriate.

47. The risk management policies and procedures must keep pace with the changing environment. The board or its designated committee(s) must review the risk management policies and key risk management procedures on a regular basis (e.g. at least annually). If the review is carried out by the board's committee(s) or senior management, any material amendment to the policies and procedures must be approved by the board.

48. When appropriate, the risk management policies and procedures must also cover the use of risk-mitigation techniques (e.g. hedging, buying insurance protection or using credit derivatives). If a bank employs risk-mitigating techniques, it must understand the risk to be mitigated and the potential effects of that mitigation (including its effectiveness and enforceability), and have in place appropriate measures to control the risks associated with these techniques.

B. Risk limits

49. A set of limits must be put in place to control a bank's exposures to various quantifiable risks associated with its business activities (e.g. credit risk, market risk, interest rate risk / profit rate risk and liquidity risk). Limits must also be used to control distinct sources of risk concentration, including (i) those arising directly from exposures to borrowers and obligors or indirectly through investments backed by a particular asset type, e.g. collateralised debt obligations, and (ii) those resulting from similar exposures across distinct business activities. These limits must be documented and approved by the board or its designated committee(s).

50. Risk limits must be set in line with a bank's risk appetite. To ensure consistency between risk limits and business strategies, the board may wish to approve limits as part of the overall annual budget process.

51. Risk limits must be suitable for the size and complexity of a bank's business activities and compatible with the sophistication of its products and services and must not merely seek to meet the minimum regulatory requirements or the general market practices. Excessively high limits fail to trigger prompt management action while overly restrictive limits that are frequently exceeded may undermine the purpose of the limit structure. Risk limits must not be overly complicated, ambitious or subjective.

52. Risk limits must be set at various levels, e.g. individual business lines or units, the entity or the group as a whole. A bank must have a clearly documented methodology for allocating overall risk limits across business lines and units.

53. The board or its designated committee(s) must ensure that limits are subject to regular review and are reassessed in the light of changes in market considerations or business strategies.

54. Risk limits must be clearly communicated to the business units and understood by the relevant staff.

55. Limit utilisation must be closely monitored. Any excesses or exceptions must be reported promptly to the chief risk officer and the senior management for necessary action.

C. New products and services

56. A bank must have an effective mechanism in place to ensure that all products and services launched are subject to proper assessment and approval procedures before launch. There must be an internally approved and clearly documented "new product approval policy" which addresses not only the development and approval of entirely new products and services but also significant changes in the features or risk profile of existing products and services. (See **Attachment B**)

57. The new product approval policy of a bank and any revisions to it must be approved by the board (or its designated committee with the necessary delegated authority). The policy must, at a minimum, cover the following areas: -

a. all aspects of the decision to enter new markets or new areas of business or to deal in new products or services, including the definition of new product, market, service or business to be adopted by the bank;

b. the internal functions to be involved in the decision;

c. other issues involved in undertaking a new activity. These may relate, for example, to pricing models, profit margin, software and technology, risk management tools, and control procedures; and

d. the process and procedures for approving significant changes to existing products or services. In general, such process and procedures must be in line with those for approving new products or services, and any simplification must be suitably justified.

58. Proposals to introduce new products or services must generally include: -

a. a description of the new product or service, and its target customers and underlying objective (e.g. for meeting customer demand, allowing the bank to better hedge its risks);

b. a detailed risk assessment, including whether the new product or service is within the bank's risk appetite, implications for the bank's risk profile (for example, in terms of credit, market, interest rate / profit rate, liquidity, operational, reputation, strategic, legal and compliance risks) and possible risk transformation if the new product or service is launched (e.g. the use of a hedging instrument to hedge the risk of a new product may result in other risks);

c. a cost and benefit analysis;

d. consideration of the related risk management implications and identification of the resources required to ensure effective risk management of the product or service (e.g. risk mitigation strategies and system enhancement);

e. an analysis of the proposed scale of new activities in relation to the bank's overall financial condition, including its capital strength and liquidity resources; and

f. the procedures to be used for measuring, monitoring, controlling or mitigating and reporting the risks.

59. All relevant functions, e.g. risk management, accounting, operations, legal and compliance, information technology must be consulted (for instance through a new product committee established within the bank), before a new product or service is launched. Such functions must ensure that the risks associated with the new product or service are adequately addressed from their respective perspectives before sign-off. The chief risk officer must escalate and report to the board (or its designated committee(s)) if there is any significant concern (e.g. material impact on the bank's risk profile) with regard to any new product or service before its launch.

60. A bank must perform a comprehensive post-implementation evaluation of new products or services (as well as existing product or services following any significant changes to their features or risk profile) to ensure no risk remains unidentified or unaddressed. The evaluation results must be taken into account for the development or any similar products or services (adopting a risk-based approach as appropriate).

61. The chief risk officer must have a holistic oversight of the risks to the bank associated with new products and services and the related risk management function must monitor and participate in the process of approving new products or services or significant changes to existing products or services) and must maintain a centralised list of approved products and services.[9] It should have a clear overview of the roll-out of new products or services (or significant changes to existing products or services) across different business units. The risk management function must also be responsible for determining whether a new initiative must be classified or categorised as a new product/service and have the authority to require that significant changes to existing products or services go through the bank's formal approval process applicable to new products or services.

62. The internal audit function must undertake regular reviews of the new product approval process encompassing the business units as well as the risk management and internal control functions involved in the process.

[9] If a centralised list of approved products and services is maintained and updated by another function, there must be appropriate arrangements to ensure that the risk management function is provided with the updated list.

V. RISK MANAGEMENT SYSTEMS AND PROCESSES

A. Risk management function

Key responsibilities and attributes

63. A bank must establish a dedicated risk management function to carry out day-to-day risk management activities across the whole organisation.

64. An effective risk management function must: -

a. have clearly defined responsibilities and accountability;

b. have a direct reporting line to senior management and direct access to the board or its risk committee;

c. be independent from the risk-taking and operational units the activities of which it reviews, and have unfettered access to information from these units that is necessary for carrying out its duties;

d. be supported by an effective management information system; and

e. be given adequate authority, management support and resources to perform its duties, and be staffed by persons with relevant expertise and knowledge.

65. The responsibilities of a bank's risk management function include: -

a. ensuring that all relevant risks of the bank are properly identified and well-understood, measured and assessed; avoided, mitigated and/or controlled, as appropriate; monitored, and reported. This will include establishing a process, using effective risk measurement techniques and management information systems, for monitoring and reporting on the bank's risk profile and its consistency with the bank's risk appetite and strategic and business plans;

b. conducting periodic reviews on the bank's risk governance arrangements, and ensuring that the bank's risk management framework (including the bank's risk appetite framework) and all related policies and control procedures are adequately implemented and working effectively;

c. being actively involved, at an early stage, in the bank's decision-making on business strategies and developments that may have implications for risk management;

d. monitoring (e.g. through an early warning or trigger system) the use of risk limits and ensuring that the risk limits are consistent with the bank's risk appetite. This will include ensuring that the risk exposures of individual business units in respect of various risks are properly aggregated and monitored against the aggregate limits for the bank as a whole;

e. overseeing and approving risk assessment models and internal rating systems (where applicable), and analysing the risks of new products and services (and of significant changes to existing products and services) and exceptional transactions;

f. conducting stress tests to assess the risk profile of the bank under stressed conditions and reporting the results of the stress tests to the board (and/or its risk committee) and senior management. The results must also be incorporated into the bank's relevant risk management and business processes (e.g. review of the bank's risk appetite, capital planning, budgeting, establishment of contingency plans);

g. providing accurate, reliable and comprehensible risk information to the board, risk committee and risk information to the board, risk committee and senior management and ensuring that all identified risk management issues or concerns (together with any proposed risk-mitigating actions) are promptly reported to them; and

h. alerting the board, risk committee and senior management to any other matters that may have a significant impact on the bank's financial position and risk profile (e.g. engagement in high-risk activities that are not aligned with the bank's risk appetite).

Chief risk officer (CRO)

66. A bank is expected to appoint a person to be responsible for the risk management function, commonly known as the CRO, who must also coordinate the risk management activities of other units within the organisation. It is generally expected that the CRO will be part of the senior management team, and his/her appointment (or cessation of appointment) will be approved by the board (or its designated committee) and publicly disclosed. In exceptional cases where, for example, a bank's size and complexity do not justify specifically appointing a person for such responsibility, one of the senior managers (such as the person in charge of internal control) may share this responsibility, provided that the roles are compatible and do not weaken checks and balances within the bank.

67. The CRO must have skills and experience which are relevant and appropriate to the nature and complexity of a bank's business activities. Moreover, he must have sufficient independence, authority and stature to enable him to challenge any proposal or decision from the risk management perspective. In this regard, the CRO must have unfettered access to any information necessary to perform his duties. The CRO must have duties distinct from other executive functions and must not have management or financial responsibility related to any business lines or revenue-generating functions.

68. The CRO must have a direct reporting line to the bank's chief executive officer (CEO) and must also report directly (without the presence of executive directors and the senior management where appropriate) to the board or its risk committee regularly and when necessary on risk management issues. In particular, he/she must play a key role in enabling the board, risk committee and senior management to understand the bank's evolving risk profile against the approved risk appetite, and must report to the board and risk committee promptly on any material breach or risk limits and any adverse development that may result in the bank's risk appetite being exceeded. The performance and remuneration of the CRO must be reviewed and approved by the board (or its designated committee).

69. As part of his/her responsibilities for the bank's risk management function, among other things, the CRO must ensure that prompt action is taken when any material risk exposure is close to or exceeds, the bank's approved risk appetite and relevant risk limits. Furthermore, the CRO must participate in key decision-making processes (e.g. strategic planning, capital and liquidity planning, new products and services approvals, remuneration design and operation) and must be involved in the setting of risk-related performance indicators for business units.

B. Risk management information system[10]

70. A bank must establish and maintain a management information system with adequate technological support and processing capacity (even in times of stress) to effectively capture, aggregate and report on the risks of major business activities within the organisation. The risk data aggregation and risk reporting framework and any substantial change to them should be reviewed and approved by the board (or its risk committee) and senior management.

71. The level of sophistication of a bank's risk management information system must be commensurate with the nature, scale and complexity of the bank's business activities. Generally, to support decision-making at different levels and enable early identification of emerging risks, it must be capable of: -

a. Accurately and reliably capturing, aggregating and reporting risk data in a timely manner, not only in normal times but also in times of stress. While different types of data will be required at different intervals, the system must be able to generate any necessary data rapidly in times of stress;

b. Capturing, aggregating and reporting risk data on all sources of relevant risks on a range of bases, including by business line, product, portfolio, function, and at entity and group levels;

c. Supporting customised identification, aggregation and reporting of risks (e.g. based on individual or a set of closely related risk drivers) to meet request of the board, senior management and other users, including AMBD;

d. Incorporating changes arising from regulatory requirements and new business developments as and when necessary;

e. Supporting a broad range of risk management analysis, including but not limited to: -

   i. incorporating multiple perspectives of any particular risk exposure to account for changes in assumptions and uncertainties in risk measurement;

   ii. incorporating hedging and other risk-mitigating actions to be carried out on a firm-wide basis while taking into account various related basis risks;

   iii. reporting excesses in limits and policy exceptions, and alerting management of risk exposures approaching pre-set limits;

   iv. facilitating the allocation of capital charges to business activities according to the level of risk-taking;

   v. conducting variance analysis against annual budget or business targets, and calculating risk-adjusted performance;

[10] This section serves to provide some general guidance for application to all banks (albeit on a proportionate basis), having regard to the BCBS pronouncement entitled "Principles for effective risk data aggregation and risk reporting" issued in 2013. A higher standard is expected of a systemically important bank. Such a bank must be able to demonstrate that it is in full compliance with Principles 1 to 11 of the "Principles for effective risk data aggregation and risk reporting" within three years of its designation.

vi. providing adequate system support for fair valuing exposures; and

vii. conducting sensitivity analysis and stress-testing and generating forward-looking firm-wide scenario analyses on evolving market conditions and stressed conditions.

72. Risk management reports must communicate information in a clear and concise manner, but yet be comprehensive enough to be useful for informed decision-making and risk assessment. Frequency, timeliness, contents, granularity, distribution and level of confidentiality of risk management reports must be appropriate for the needs of recipients. While an individual bank must determine risk reporting requirements that are appropriate for its own business models and risk profiles, at a minimum, the reports must cover all material risk areas (e.g. credit, market, interest rate / profit rate, liquidity, operational, reputation, legal and strategic risks) and provide information in respect of risk concentrations, adherence to risk appetite and risk limits and forward-looking assessment of risks. In addition, the risk management reports must provide information relating to regulatory ratios (e.g. capital adequacy ratios and liquidity ratios) and their projections.

73. There must be proper control, validation and reconciliation processes in place to ensure the accuracy of risk management reports, and relevant processing must be documents with appropriate explanation. For instance, it is expected that risk data aggregation must occur on a largely automated basis. There must be automated and manual checks, including validation rules to help verify data inputs and calculations. Risk data and reports must be reconciled with other relevant sources (e.g. accounting data and reports) where appropriate. The risk management reports must meet the accuracy requirements set by the senior management for different types of reporting (e.g. some data requires a high degree of precision while a certain extent of approximation may be allowed for information generated from models and stress testing).

74. To remain effective, there must be processes to identify, rectify and alert the senior management (where appropriate) of any incompleteness, exception, limitation and weakness of the bank's risk management information system in capturing, aggregating and reporting of risks. The system must also be subject to regular review and enhancement. Moreover, the capabilities of the bank's risk management system must be considered by the board (or its risk committee) and senior management as part of any approval process for new initiatives (e.g. development of new products and acquisition) and a clear timeframe must be set for making any required upgrading or adjustment.

C. Risk measurement and assessment

75. A bank must employ effective methodologies and tools for the measurement of various types of quantifiable risk and for the assessment of other risks which are not easily quantifiable (e.g. reputation risk).

76. Different methods or models may be used to assess or measure each type of risk. In determining the methods or models to be adopted for risk measurement or assessment, a bank must, among other things, consider the following factors: -

a. the nature, scale and complexity of its business activities;

b. its business needs (e.g. for pricing);

c. the assumptions underpinning the methods or models;

d. data availability;

e. the sophistication of its management information system; and

f. staff expertise.

77. The board or its designated committee(s) and senior management must recognise the biases and assumptions embedded in, and the constraints of, the methods or models chosen (including associated valuation and pricing methodologies) in order to better assess the results generated from those methods or models. They must also satisfy themselves as to the adequacy and appropriateness of the key assumptions, data sources and procedures used to measure or assess the risks.

78. The accuracy and reliability of a risk measurement method or model must be verified against the actual results through regular back-testing. The measurement method or model (including the underlying assumptions) must also be subject to periodic update to reflect changing market conditions.

79. A bank must avoid over-reliance on any specific risk methodology or model. Modeling and risk management techniques must always be tempered by expert judgement. For example, models that project very high returns on economic capital may arouse concern as to whether this is in fact caused by a deficiency in the models (such as failure to take into account all relevant risks). Where practicable, a bank must use a range of risk measures or tools to provide different views of risk on the same exposures.

80. Similarly, decisions which determine the level of risks to be taken must not only be based on quantitative information or model outputs but must also consider the practical and conceptual limitations of the methods and models adopted, using a qualitative approach which includes expert judgement and critical analysis. In addition, relevant macroeconomic trends and data must explicitly be addressed to identify its potential impact on particular business activities. Such assessments must be formally integrated into material risk decisions.

81. A bank must use stress tests to complement risk management models that are based on complex quantitative models using backward-looking data and estimated statistical relationships. In particular, stress-testing outcomes for a specific portfolio can provide insights about the validity of statistical models at high confidence intervals. However, banks must recognise that stress-testing results are highly dependent on the limitations and assumptions of the scenarios used, namely the severity and duration of the shock and the underlying risks.

82. For risk measurement purposes, a bank must be able to value its positions (including those associated with complex products and financial instruments) based on sound valuation practices. This must be the case both in normal times and in times of stress. For exposures that represent material risk, a bank must have the capacity to produce valuations using alternative methods in the event that primary inputs and approaches become unreliable, unavailable or irrelevant due to market disruptions or illiquidity.

D. Risk-adjusted performance measurement

83. A bank is expected to adopt a system for measuring the performance of its business units on a risk-adjusted basis to enable them to compare the financial performance of individual business units, considering the risks associated with their activities and any breaches of risk limits or other risk management measures. This ensures that business units are not rewarded for taking on excessive risks.

84. To enable efficient allocation of capital and other financial resources to individual business units and to provide these units with incentives for controlling the risks generated from their activities, the performance measurement system (including internal pricing mechanisms) used by banks must be able to comprehensively measure the risks associated with the units' business activities. Management information systems must be able to attribute risk and earnings to their appropriate sources and to measure earnings against capital allocated to the activity, after adjusting for various risks (such as the expected loss on credit facilities).

85. Data inputs and information used for the purpose of calculating remuneration payable to a bank's senior management and staff must be subject to independent review to ensure appropriateness and accuracy.

E. Sensitivity analysis and stress-testing

86. A bank must have adequate systems and capability to measure the sensitivity of earning to a change in individual risk factors (e.g. interest rates / profit rates) and conduct stress tests to: -

a. identify possible events or market changes that could have serious adverse effects or a significant impact on their overall risk profiles and financial positions;

b. address existing or potential risk concentrations; and

c. facilitate the development of risk mitigating measures or contingency plans across a range of stressed conditions.

87. The sensitivity analyses and stress tests must be conducted regularly on major business activities, and on a firm-wide basis. Stress scenarios must be comprehensive and forward-looking and include risk factors that can significantly affect a bank or its individual business units.

88. The board (or its risk committee) and senior management must have direct involvement in setting stress-testing objectives, defining stress scenarios, discussing the results of sensitivity analyses and stress tests, assessing potential actions and making relevant decisions. The stress-testing outcomes must be taken into account in the setting of policies and limits.

VI. INTERNAL CONTROLS, AUDITS AND CONTINGENCY PLANNING

A. Internal control systems[11]

89. A critical element to support an effective risk management framework is the existence of a sound internal control system.

90. A properly structured internal control system must: -

a. help to promote effective and efficient operation;

b. provide reliable financial information;

c. safeguard assets;

d. minimise the operating risk of loss from irregularities, fraud and errors;

e. ensure effective risk management systems; and

f. ensure compliance with relevant laws, regulations and internal policies.

91. A bank's internal control system must, at a minimum, cover the following: -

a. high level controls, including clear delegation of authority, written policies and procedures, separation of critical functions (e.g. marketing, risk management, accounting, settlement, audit and compliance);

b. controls relating to major functional areas, including retail banking, corporate banking, institutional banking, private banking and treasury. Such controls must include segregation of duties, authorisation and approval, limit monitoring, physical access controls, etc.;

c. controls relating to financial accounting (e.g. reconciliation of nostro accounts and review of suspense accounts), annual budgeting, management reporting and compilation of prudential returns to the regulators;

d. controls relating to financial technology;

e. controls relating to outsourced activities[12], where applicable; and

f. controls relating to compliance with statutory and regulatory requirements (including but not limited to those relating to anti-money laundering and counter-terrorist financing).

92. An effective internal control system requires a strong control environment[13] to which the board and senior management provide their full support, and an internal audit function to evaluate

[11] Refer to AMBD's Guidelines on Internal Control Systems (Guidelines No. BU/G-7/2018/15), dated 2nd January 2018 as may be revised from time to time.

[12] Refer to AMBD's Outsourcing Guidelines, dated 7th September 2012 as may be revised from time to time.

[13] "Control environment" means the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance in the entity.

its performance on a regular basis.

B. Compliance function[14]

93. The compliance function plays an important role with respect to a sound risk management framework but must not be regarded as a substitute for regular and adequate internal audit coverage. The work of the compliance function must be subject to periodic reviews by the internal audit function.

94. The primary role of a bank's compliance function is to assist the bank to ensure compliance with the statutory provisions, regulatory requirements and codes of conduct applicable to its banking or other regulated activities. This includes ensuring that the bank has appropriate internal policies to achieve compliance. (For the avoidance of doubt, the responsibility for achieving compliance does not rest only with the compliance function but every function and staff of a bank have its respective responsibility for ensuring compliance.)[15]

95. Key responsibilities of the compliance function include[16]: -

a. Identifying, assessing and monitoring compliance risk;

b. advising senior management on the laws, rules and standards (and any changes of such) with which the bank is required to comply;

c. establishing the bank's compliance policies and guidelines and ensuring that they remain effective;

d. providing compliance-related advice and training to staff;

e. reporting regularly to, and advising senior management on, compliance matters; and

f. establishing a compliance program that sets out its planned activities, including the scope of review of policies and procedures to ensure that the bank's compliance with applicable statutory provisions, regulatory requirements and codes of conduct.

96. A bank is expected to have an independent compliance function and to appoint a person (commonly known as the head of compliance or chief compliance officer (CCO)) to be responsible for the firm-wide compliance function or, in the case of a foreign bank, the compliance function of its local operations. The appointment of the CCO must be approved by the board (or its designated committee). A bank must promptly and in any event, within 14 days, notify AMBD of the appointment (and cessation of appointment) of its CCO.

97. In exceptional cases where, for example, a bank's scale of operations may not justify having all necessary tasks carried out internally by the compliance function, other arrangements

[14] Refer to AMBD's Guidelines on Compliance and Compliance Function (Guidelines No. BU/G-5/2018/13), dated 2nd January 2018 as may be revised from time to time.

[15] A bank must note that non-compliance with other areas not directly related to banking or regulated activities (e.g. breach of labor or company laws) could also give rise to legal or regulatory sanctions, material financial loss, or loss of reputation. If not the bank's compliance function, there must be other parties, such as the bank's legal function, responsible for providing advice on, or monitoring the legal implications associated with, such areas.

[16] If some of these responsibilities (e.g. legal advice on laws, rules and standards)are carried out by staff in other functions, the allocation of responsibilities to each function must be clear.

(such as hiring an external lawyer to provide legal advice on a need basis or an appropriate allocation of duties among functions) may be acceptable. In any case, where certain tasks of the compliance function are outsourced, there must nevertheless be adequate oversight by the bank's CCO.

98. An effective compliance function must: -

a. have adequate resources and be staffed by an appropriate number of competent staff who are sufficiently independent of the business and operating units. The CCO and the staff of the compliance function must not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have;[17]

b. be given appropriate standing and authority within the bank. It must report to a designated committee of the board (e.g. the audit committee) or senior management and have the right to report matters to the board directly as necessary; and

c. be able to carry out its duties on its own initiative in all business and operating units of the bank in which compliance risk exists, with unfettered access to any records or files necessary to enable it to conduct its work.

99. To ensure effective management of compliance risk, the bank's compliance policy must document the organisation, status and responsibilities of the compliance function as well as other measures to manage compliance risk. The board must approve the policy and must oversee the implementation of the policy by senior management (with the assistance of the compliance function) through regular review of the extent to which the policy is observed. The board may designate an appropriate board-level committee to review and approve the compliance policy and conduct regular reviews of how the policy is being implemented. In such a case, the designated committee (e.g. the audit committee) must have the required independence to take up the mandate. The board must monitor the committee's performance to ensure that its directives are properly followed[18].

C. Internal audit function[19]

100. A bank's internal audit function must, among other things, perform independent periodic checking on whether the risk management framework approved by the board is properly implemented and the established policies and control procedures in respect of risk management are complied with.

101. The effectiveness of a bank's risk management processes and related internal controls must be assessed and tested periodically. The scope and frequency of audit may vary but must be increased if there are significant weaknesses or major changes or new products or services are introduced.

[17] For instance, among other things, the CCO must not have responsibilities for any business units of the bank. Remuneration of the CCO and the staff of the compliance function must not be influenced by, or linked to the performance of, the business and operational units which are subject to monitoring by the compliance function.

[18] In the case of a foreign bank operating a branch in Brunei, the head office of the bank many authorise the branch to establish the compliance policy for the local operations, provided that the policy is approved by the head office before it is implemented and there is a process for the head office to oversee how the policy has been implemented.

[19] Refer to AMBD's Guidelines on Internal Audit Function (Guidelines No. BU/G-3/2018/11), dated 2nd January 2018 as may be revised from time to time.

102. In fulfilling its responsibilities relating to a bank's risk management, the internal audit function must, among other things, assess (on a group basis and on the basis of individual business units and legal entities) and report to the board (or its audit committee) periodically whether: -

a. the bank's risk governance arrangements and risk appetite framework are effective, both in their design and operation (including the linkages to the bank's risk culture, strategic and business planning, remunerations and decision-making processes);

b. breaches of risk limits are being appropriately identified, escalated and reported;

c. the bank's risk measurement techniques and risk management information system and related reporting are effective; and

d. the bank's reporting system is effective.

103. All material risk management deficiencies and weaknesses (including any non-compliance with internal policies and procedures as well as stipulated regulatory requirements on risk management) identified must be directly and promptly reported to the board (or its audit committee) and senior management for early rectification.

104. A bank must have in place appropriate arrangements (such as periodic meetings) to facilitate effective exchange of information between the audit committee and risk committee, and to ensure that all material risks and related risk management processes are subject to independent assessment by the internal audit function.

D. Contingency, business continuity and recovery planning

105. Each bank must, as part of its business continuity planning, contingency funding planning and recovery planning, ensure that the bank's risk management function will be able to fulfil its roles and responsibilities effectively in emergency and crisis situations. A bank must subject its contingency, business continuity and recovery arrangements to annual and ad hoc review (when circumstances dictate the need for ad hoc reviews) and commissioning triennial independent reviews. A bank must submit such a review to the AMBD within one month of completion thereof.

VII. GLOSSARY

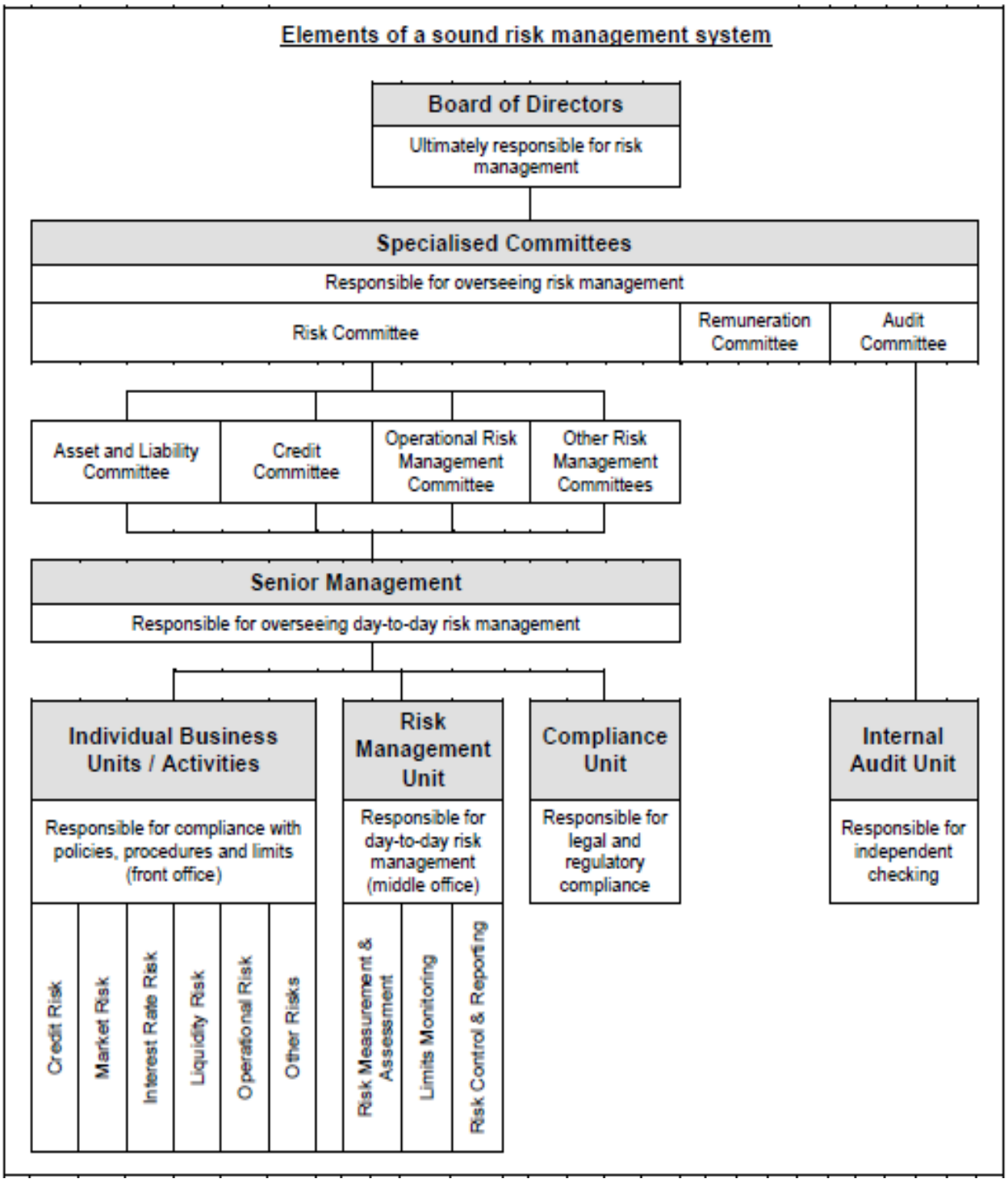
For the purposes of these guidelines, the following terms will have the following meanings:

TERM	MEANING
AMBD	Autoriti Monetari Brunei Darussalam as defined by the Autoriti Monetari Brunei Darussalam Order, 2010 [S 103/10]
Bank	A company which carries on banking business and holds a licence granted under section 4 or section 23 of the Banking Order 2006, or the Islamic Banking Order, 2008
Basel Core Principles or BCPs	the Basel Committee on Banking Supervision pronouncement titled *Core Principles for Effective Banking Supervision, 2012*, (bcbs230).
board	board of directors
CCO	chief compliance officer
CEO	chief executive officer
CFO	chief financial officer
CRO	chief risk officer
Risk	negative outcomes in the form of (financial and non-financial) losses incurred by a bank or banking group arising from future outcomes and impacting its financial performance and financial position.
Risk appetite	a component of the risk management framework and means, in relation to a bank: - 1. The nature, types and aggregate level of risk a bank is willing to assume, decided in advance, and within its risk capacity, to achieve its strategic objectives and business plan. 2. A high-level determination of how much risk a bank is willing to accept, taking into account the risk/return attributes. It is often a forward-looking view of risk acceptance. Risk appetite may include both quantitative and qualitative elements.

Risk appetite framework (RAF)	the overall approach, including policies, processes, controls and systems through which risk appetite is established, communicated and monitored. It includes a risk appetite statement, risk limits and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the RAF. The RAF must consider material risks to the bank, as well as to its reputation vis-a-vis depositors, investors and customers. The RAF aligns with the bank's strategy.
Risk appetite statement (RAS)	in relation to a bank, a board-approved formal written articulation of the nature and extent of the types and levels of risk which a bank will accept, mitigate or avoid in order to achieve its business objectives. The board of directors must approve and review a risk appetite and tolerance statement that articulates the nature, types, and levels of operational risk that the bank is willing to assume.
Risk (management) culture	in relation to a bank: - 1. Means a culture which supports and provides appropriate standards and incentives for professional and responsible behavior throughout the whole organisation. 2. Is constituted of the bank's norms, attitudes and behaviors related to risk awareness, risk taking and risk management and controls that shape decisions on risks, influence the decisions of management and employees during day-to-day activities, and is reflected in the risks they assume. 3. Is constituted of the combined set of individual and corporate values, attitudes, competencies and behavior that determine a bank's commitment to and style of risk management. 4. Is based, inter alia, on a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts of interest. 5. Sets clear expectations and accountabilities to ensure that bank staff understand their roles and responsibilities for risk as well as their authority to act.

Risk (management) framework	collectively, the systems, structures, policies, procedures and people that identify, measure and evaluate, control and mitigate, monitor, and report risk on a bank-wide (and group-wide) basis.
Risk profile	in relation to a bank, a point-in-time assessment of the bank's gross (before the application of any mitigants) or net (after taking into account mitigants) risk exposures aggregated within and across each relevant risk category based on current or forward-looking assumptions. A target / desired risk profile is a management tool which can be useful to compare to the actual risk profile.

ATTACHMENT A. Example of a risk management organogram



Note: The illustration is not intended to be prescriptive.

ATTACHMENT B. Examples of significant changes in features or risk profile

Examples of significant changes in features or risk profile of products and services.

A) Treasury-related

Feature changed	Original	New	Reason
Product feature(s)	1. European call option on index 2. Treasuries up to 5-year tenor 3. Trading of off-shore Korean Won 4. European option on HSI	1. European call option on single stocks 2. Treasuries up to 30-year tenor 3. Trading of on-shore Korean Won 4. American option on HSI	The risk profiles (e.g. liquidity risk, market risk, regulatory risk, etc.) of the products have changed significantly
Hedging strategy	Fully back-to-back to an interbank counterparty	Market risks warehoused under limits	Risk profile has changed significantly
Role of service provision	Stock dealing in primary market	Prop-trading stocks	Role of service provision has changed, impacting approach to risk management

B) Others

- Product re-launch after a substantially long lapse (e.g. market conditions or regulatory requirements have changed.)
- Product pass-through to customers versus position taking by a bank itself.
- Change in markets (e.g. different geographical locations involving different legal or regulatory requirements, and different liquidity and volatility risks).
- Change in distribution channel (e.g. mobile banking and internet banking.
- Change in counterparty or customer segment targeted by the product (e.g. from interbank counterparty or large institutional clients to high net worth individuals or retail customers, who may not possess the same level of expertise to assess the risks and returns of the same products).
- Change in currency denomination of an existing product.
- Change in market positioning (e.g. end user, active player and market maker).
- Change in platform (e.g. over-the-counter, exchange and electronic).
- Change in process (e.g. automation).
- Change in booking arrangements (e.g. from held-to-maturity to trading).

- Change in settlement methodology (e.g. from physical delivery to cash settlement).

- Major changes in documentation including legal documents (e.g. margining requirement and netting arrangements).

- **END** -