This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To specify the key elements of a risk management framework which the MA expects AIs to have in place.

Classification

A ~~statutory~~ guideline issued by the MA under §7(3) of the Banking Ordinance (BO), ~~§7(3)~~.

Previous guidelines superseded

IC-1 "General Risk Management Controls" (V.1) dated 25.04.03, ~~and~~ (V.2) dated 31.12.2010 and (V.3) dated 06.10.2017.

Application

To all AIs.

Structure

1. Introduction
   - 1.1 Background
   - 1.2 Application
2. Key elements of an effective risk management framework
   - 2.1 Risk governance
   - 2.2 Risk appetite framework
3. Responsibilities of the Board and senior management
   - 3.1 Overall responsibilities
   - 3.2 Setting of risk appetite and monitoring
   - 3.3 Firm-wide risk management

3.4 Use of specialised committees

4. Risk management policies, procedures and limits
   - 4.1 Policies and procedures
   - 4.2 Risk limits
   - 4.3 New products and services

5. Risk management systems and processes
   - 5.1 Risk management function
   - 5.2 Risk management information system
   - 5.3 Risk measurement and assessment
   - 5.4 Risk-adjusted performance measurement
   - 5.5 Sensitivity analysis and stress-testing

6. Internal controls, audits, ~~and~~ contingency planning and reporting and notification requirements
   - 6.1 Internal control system
   - 6.2 Internal audit function
   - 6.3 Compliance function
   - 6.4 Contingency, business continuity and recovery planning
   - 6.5 Reporting and notification requirements

1. Introduction

1.1 Background

1.1.1 Risk-taking is an integral part of banking business. Each AI has to find an appropriate balance between the level of risk the AI is willing and able to take and the level of return it seeks to attain, without undermining its overall financial soundness and viability. An effective risk management framework, that is commensurate with the size and complexity of an AI's operations, needs to be in place to help ensure that risks are well managed within the AI's risk appetite and that the necessary systems and controls achieve their intended results.

1.1.2 According to the "Core Principles for Effective Banking Supervision" issued by the Basel Committee on Banking Supervision ~~in September 2012~~ ("Basel Core Principles"), banking supervisors should be satisfied that banks 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.

1.1.3 Consistent with the Basel Core Principles, the HKMA requires AIs, under its risk-based supervisory approach, to establish a sound and effective system to manage each of the eight inherent risks (viz. credit, market, interest rate, liquidity, operational, reputation, legal and strategic) to which they are exposed (see SA-1 "Risk-based Supervisory Approach"). ~~Locally incorporated~~ AIs incorporated in Hong Kong are also required to have adequate internal systems for assessing capital adequacy in relation to the risks they assume (as prescribed in CA-G-5 "Supervisory Review Process").

1.1.4 This module is intended to set out the HKMA's expectations in respect of AIs' risk management frameworks. Some of the specific systems and controls

associated with various inherent risks are separately described in other modules.[1]

1.2 Application

1.2.1 The standards in this module will be applied to AIs on a proportionate basis, having regard to their size, nature and complexity of operations. Thus, AIs 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 and complex AI. In general, ~~locally incorporated~~ AIs incorporated in Hong Kong should apply these standards on the solo-entity basis and, where applicable, the consolidated basis covering their subsidiaries and, to the extent practicable, associated companies and joint ventures which may expose them to significant potential risk.[2] International banking groups operating in Hong Kong (whether in the form of a local subsidiary or a branch) should have a local risk management framework appropriate for their Hong Kong operations. If certain risk management functions pertaining to a banking group's Hong Kong operations are centralized at the group or regional level, the AI, upon request by the HKMA, should be able to demonstrate that the relevant functions performed at the group or regional level are appropriate for the size, nature and complexity of the local operations and are in line with the standards in this module in all material aspects.

1.2.2 Failure to adhere to the standards set out in this module may call into question whether an AI continues to satisfy the minimum criteria for authorization in the ~~Banking~~

---

1 For example: CR-G-1 "General Principles of Credit Risk Management"; CR-G-13 "Counterparty Credit Risk Management"; TA-2 "Foreign Exchange Risk Management"; IR-1 "Interest Rate Risk Management"; LM-2 "Sound Systems and Controls for Liquidity Risk Management"; OR-1 "Operational Risk Management"; RR-1 "Reputation Risk Management"; and SR-1 "Strategic Risk Management".

2 Whether the standards should be applied to associated companies or joint ventures will also depend on the extent of an AI's affiliation to the entities and the level of control it can exercise over the entities.

~~Ordinance (BO)~~ and cast doubt on the fitness and propriety of the AI's directors, chief executives and other members of its senior management.

2. Key elements of an effective risk management framework

2.1 Risk governance

2.1.1 Risk governance refers to the formal arrangements that enable the Board of Directors (the Board) and senior management of an AI to establish sound business strategy, articulate and monitor adherence to risk appetite and risk limits, and identify, measure, manage and control risks.

2.1.2 To ensure effective risk management, an AI should have in place a set of robust risk governance arrangements, whereby responsibilities of the Board and senior management, and among different functions of the AI (and the respective risk owners), are well defined. The risk governance framework should also outline escalation and notification procedures (including vertically to the Board and senior management) as well as potential disciplinary actions for excessive risk-taking by individuals.

2.1.3 It is generally expected that responsibilities among different functions of the AI are defined in such a way that there are three lines of defence which are independent from each other:

- the first line of defence is provided by the business units where risks are taken. In the course of conducting business activities, staff in the business units hold frontline positions in the proper identification, assessment, management and reporting of risk exposures on an ongoing basis, having regard to the AI's risk appetite, policies, procedures and controls. The roles and

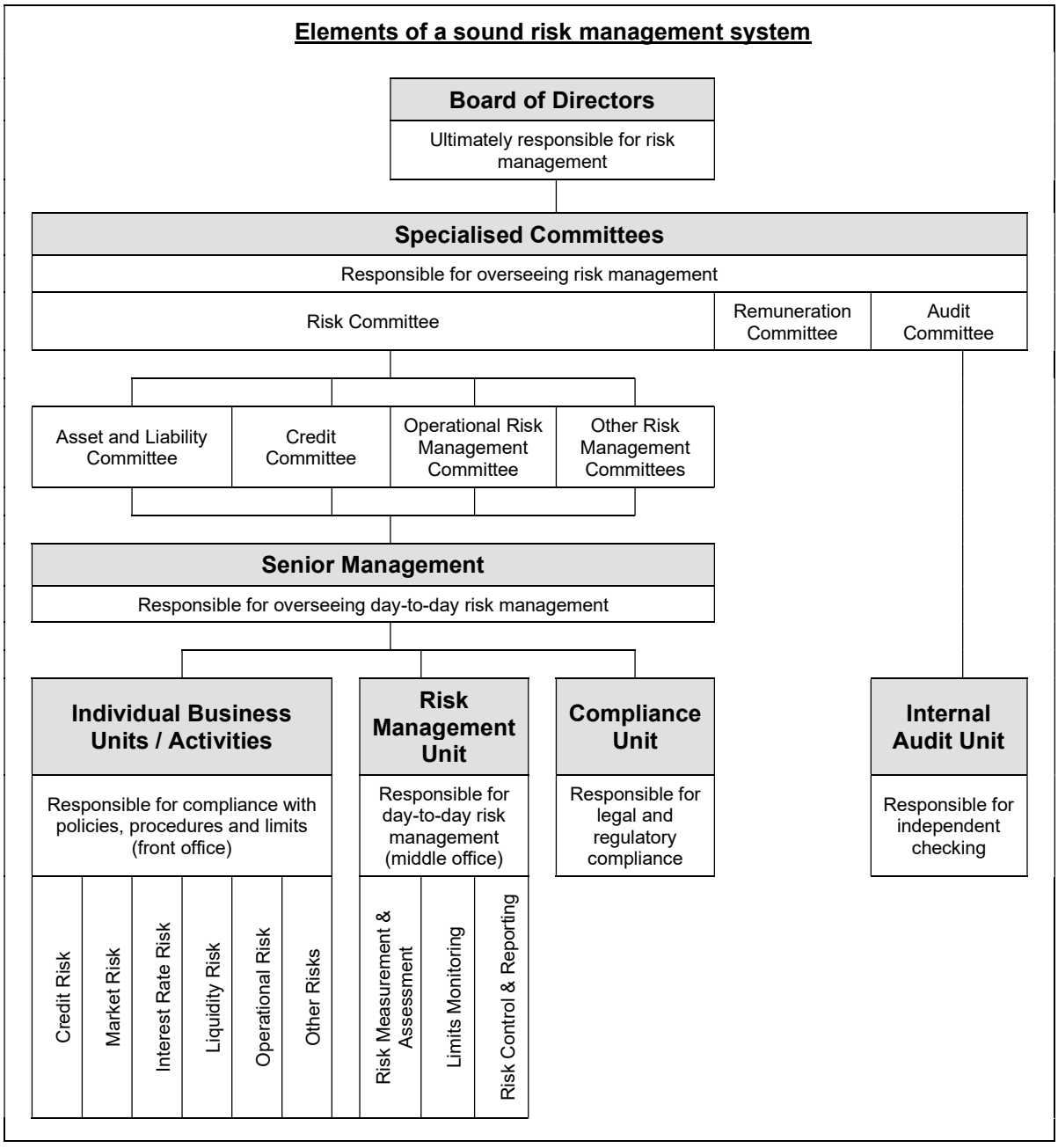
responsibilities of risk owners in business units should be clearly defined[3];

- the second line of defence is provided by independent and effective risk management and compliance functions. The risk management function is primarily responsible for overseeing the AI'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

- 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 AI's risk management framework including the risk governance arrangements (including the first and second lines of defence described above).

2.1.4 An overview of how these elements fit together is illustrated below, although this illustration is not intended to be prescriptive.

[3] For instance, the person heading a business unit, as a risk owner, should ensure that activities of the unit are in line with the AI'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.


Elements of a sound risk management system
Board of Directors
Ultimately responsible for risk management
Specialised Committees
Responsible for overseeing risk management
Risk Committee
Remuneration Committee
Audit Committee
Asset and Liability Committee
Credit Committee
Operational Risk Management Committee
Other Risk Management Committees
Senior Management
Responsible for overseeing day-to-day risk management
Individual Business Units / Activities
Responsible for compliance with policies, procedures and limits (front office)
Credit Risk
Market Risk
Interest Rate Risk
Liquidity Risk
Operational Risk
Other Risks
Risk Management Unit
Responsible for day-to-day risk management (middle office)
Risk Measurement & Assessment
Limits Monitoring
Risk Control & Reporting
Compliance Unit
Responsible for legal and regulatory compliance
Internal Audit Unit
Responsible for independent checking

2.1.5 Furthermore, effective risk governance requires a strong risk culture [4] which promotes risk awareness and encourages open communication and challenge with regard to risk-taking across the AI (including vertically to and from the Board and senior management). Obstacles that impede legitimate sharing of information across different functions within an AI (e.g. competition between, or incompatible IT systems among, business lines) should be avoided, as these obstacles may result in decisions being made in silos which may not be in the best interest of the AI as a whole. [5] Information communicated to the Board and senior management should be timely, accurate and presented in an understandable and concise format. Material risk-related information that requires immediate decision or reaction should 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.

2.1.6 Risk governance arrangements should be documented and updated as appropriate. An AI should 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.

2.2 Risk appetite framework

2.2.1 In addition to a set of robust risk governance arrangements, it is also important that an AI's risk management is underpinned by an effective risk appetite framework, which refers to the policies, processes, controls and systems, with clearly defined

---

[4] Risk culture refers to an AI's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. An AI'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.

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

responsibilities, through which risk appetite is established, communicated and monitored.

2.2.2 The risk appetite framework of an AI should be driven by leadership from the Board and senior management, supplemented as appropriate by the involvement of management at functional and affiliated entity levels, for the purpose of providing information and analysis to facilitate the assessment of risk appetite (by senior management) and the review and final approval of a risk appetite framework and statement (by the Board). The framework should facilitate the embedding of the risk appetite into the AI's risk culture. The establishment and effective implementation of a risk appetite statement and risk limits are key to a sound risk appetite framework (see subsections 3.2 and 4.2 for more details).

3. Responsibilities of the Board and senior management

3.1 Overall responsibilities

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

3.1.2 In fulfilling this responsibility, the Board and senior management should, among other things:

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

- have direct involvement in setting, and monitoring adherence to, the AI's risk appetite, which should be commensurate with its operations and strategic goals;

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

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

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

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

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

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

- ensure that the AI's remuneration systems are consistent with, and promote, effective risk management and do not incentivise imprudent or excessive risk-taking (see CG-5 "Guideline on a Sound Remuneration System");~~ and~~

- promote the establishment of regular and transparent communication mechanisms within the organisation; and

- ensure processes are in place to enable the AI to report, and notify the HKMA of, certain matters in

accordance with applicable legal and regulatory requirements (see also subsection 6.5 for details).

3.2 Setting of risk appetite and monitoring

3.2.1 The Board should develop in collaboration with the senior management and approve an AI's risk appetite framework, and ensure that it is consistent with the AI's strategic, business, capital and financial plans, as well as the AI's risk-taking capacity and remuneration system.

3.2.2 The Board is responsible for setting the AI's overall risk appetite and approving the risk appetite statement recommended by the senior management. While there is no standard means of expressing an AI's risk appetite, it should be articulated clearly and concisely to facilitate internal communication and implementation. The level of detail and sophistication of an AI's risk appetite statement should be commensurate with the AI's business nature and risk management needs. An AI's risk appetite statement should so far as practicable:

- express the AI'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;

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

- 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 AI's risk profile against its risk appetite and risk-taking capacity;

- 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;

- 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 AI's strategic and business plans; and

- be forward looking, and include appropriate financial targets that are consistent with the AI's risk appetite, and outline possible measures and actionable elements that reflect the AI'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 should be realistic and feasible for restoring capital or reducing risk in adverse situations and should not be inconsistent with the AI's recovery plan (where applicable).

3.2.3 The Board should 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 AI's risk appetite framework and its risk appetite statement. Sufficient information should be compiled to facilitate regular assessment by the Board and senior management of the management of risk against the AI's risk appetite, such as (i) relevant measures of risk (e.g. based on economic capital or stress tests); (ii) a view of how risk levels compare with limits; (iii) the level of capital that the AI would need to maintain after sustaining a loss of the magnitude of the risk measure; and (iv) the actions that management could take to restore capital after sustaining a loss.

3.2.4 The risk appetite statement should be used as the basis for the Board, senior management, business units and internal control functions to deliberate upon and formulate the AI'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 AI. 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 should ensure that there is an assessment of the AI's risk appetite in the decision-making process. In these circumstances, the Board should thoroughly understand the AI'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 AI's capital, liquidity and risk positions.

3.2.5 Any changes to the AI's risk appetite statement should be approved by the Board. The justification for change should be adequately documented.

3.3 Firm-wide risk management

3.3.1 The Board and senior management should 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

3.3.2 To ensure adequate oversight of firm-wide risks, the Board should, among other things, be responsible for:

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

- identifying, understanding and assessing the risks inherent in the AI's business activities or in new products or services to be launched (see also subsection 4.3 below);

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

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

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

- ensuring that information systems and infrastructure across all business units and control functions are sufficiently resourced and supportive of the AI's risk management and reporting needs; and

- ensuring that independent risk management and control functions are robust, truly independent from the AI'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

3.3.3 Senior management should be responsible for:

- formulating detailed policies, procedures and limits for managing different aspects of risk arising from the AI's business activities, based on the risk management strategies laid down by the Board;

- designing and implementing a risk management framework to be approved by the Board and ensuring that the relevant control systems within the

framework work as intended. The framework should 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;

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

- identifying and acting on emerging risks and, where appropriate, reporting any material risks to the Board promptly; and

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

3.4 Use of specialised committees

3.4.1 While the Board is ultimately responsible for risk management, it may be beneficial for it to delegate authority to appropriate Board-level committees (see also Section 5 of CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions", and paragraph 3.4.3 below) to carry out some of the risk management tasks described in paragraph 3.3.2 above. Delegation of authority should be made on a formal basis with a clear mandate. Appropriate reports should be submitted regularly to the Board by the committee(s) to which such authority has been delegated.

3.4.2 It should 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 members of the Board are expected to have an adequate understanding of the nature of the AI'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.[6] If existing members lack the relevant expertise, bringing in new members with such knowledge or appointing external consultants should be considered.

3.4.3 As provided in CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions", all ~~locally incorporated~~ AIs incorporated in Hong Kong, except restricted licence banks or deposit-taking companies (other than one designated by the ~~Monetary Authority~~MA under §3S or §3U of the Banking (Capital) Rules (BCR) as systemically important) with a relatively small and simple business operation and low risk profile, should establish a Risk Committee. All other ~~locally incorporated~~ AIs incorporated in Hong Kong are also strongly encouraged to do so. The Risk Committee should:

- be a stand-alone committee and distinct from the Board's Audit Committee;
- 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 should be avoided;
- be composed of a majority of members who are independent non-executive directors. Members of the Risk Committee should collectively possess relevant technical expertise and experience in risk disciplines that are adequate to enable them to discharge their responsibilities effectively;
- review and recommend for the Board's approval the AI's risk management strategies, key risk policies and risk appetite, at least annually;

[6] For example, some members should 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.

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

- review and assess the adequacy of the AI's risk management framework and policies in identifying, measuring, monitoring and controlling risks and the extent to which these are operating effectively;

- oversee the establishment and maintenance by senior management of appropriate infrastructure, resources and systems for risk management, particularly in relation to the AI's adherence to the approved risk appetite and related policies;

- 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 AI, to ensure they are consistent with the stated risk appetite;

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

- review periodic reports provided by the senior management (including the Chief Risk Officer) on the state of the AI's risk culture, risk exposure and risk management activities;

- ensure that the staff members of the AI responsible for implementing risk management systems and controls are sufficiently independent of the AI's relevant risk-taking activities; and

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

4. Risk management policies, procedures and limits

4.1 Policies and procedures

4.1.1 AIs should have clearly defined and documented policies and procedures that enable firm-wide risks to be managed in a proactive manner[7], with emphasis on achieving:

- objective and consistent risk identification and measurement approaches;
- comprehensive and rigorous risk assessment and reporting systems;
- sound valuation and stress-testing practices; and
- effective risk monitoring measures and controls.

Risk management policies and key risk management procedures should 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.

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

4.1.3 The development of risk management policies and procedures should take account of the following factors:

- an AI's overall business strategy and activities;

---

7 ~~Overseas-incorporated~~ AIs incorporated outside Hong Kong may, to a large extent, apply the firm-wide policies and procedures set by their head offices to their Hong Kong operations, provided that such documents are customised to take account of local market conditions.

- the appropriateness to the size, nature and complexity of the AI's business activities;
- the risk appetite of the AI;
- the level of sophistication of the AI's risk monitoring capability, risk management systems and processes;
- the AI's past experience and performance;
- the economic substance of the AI's risk exposures (including reputation risk and valuation uncertainty);
- the results of sensitivity analysis and stress tests;
- anticipated internal or external changes (e.g. planned operational changes or expected changes in market conditions); and
- any legal and regulatory requirements.

4.1.4 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), should be spelled out clearly in the policies and procedures, and updated as appropriate.

4.1.5 The risk management policies and procedures should keep pace with the changing environment. The Board or its designated committee(s) should 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 should be approved by the Board.

4.1.6 Where appropriate, the risk management policies and procedures should also cover the use of risk-mitigating techniques (e.g. hedging, buying insurance protection or using credit derivatives). If AIs employ risk-mitigating techniques, they should 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.

4.2 Risk limits

4.2.1 A set of limits should be put in place to control an AI's exposure to various quantifiable risks associated with its business activities (e.g. credit risk, market risk, interest rate risk and liquidity risk). Limits should also be used to control different 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 different business activities. These limits should be documented and approved by the Board or its designated committee(s).

4.2.2 Risk limits should be set in line with an AI'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.

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

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

4.2.5 The Board or its designated committee(s) should ensure that limits are subject to regular review and are reassessed in the light of changes in market conditions or business strategies.

4.2.6 Risk limits should be clearly communicated to the business units and understood by the relevant staff.

4.2.7 Limit utilisation should be closely monitored. Any excesses or exceptions should be reported promptly to the Chief Risk Officer and the senior management for necessary action.

4.3 New products and services

4.3.1 AIs should 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 should 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 Annex 1 for examples). The approach to determining whether changes to existing products and services are considered to be "significant" should also be documented.

4.3.2 The new product approval policy of an AI and any revisions to it should be approved by the Board (or its designated committee with the necessary delegated authority). The policy should, at a minimum, cover the following areas:

- 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 AI;
- the internal functions to be involved in the decision (see also paragraph 4.3.5 below);
- 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
- the process and procedures for approving significant changes to existing products or services. In general,

such process and procedures should be in line with those for approving new products or services, and any simplification should be suitably justified.

4.3.3 New products or services should be subject to a careful evaluation or pre-implementation review to ensure that:

- all relevant parties, including the Board or its designated committee(s), senior management and other managers as appropriate, fully understand the risk characteristics; the underlying assumptions regarding business models, valuation and risk management practices; the potential risk exposure if those assumptions fail; and the possible difficulty in valuing the product involved, especially in times of stress; and

- there are adequate staffing, technology and resources (financial, risk management, compliance etc.) to launch the product or service, as well as adequate internal tools and expertise to measure and manage the risks associated with it. Any material inadequacies should be properly addressed before launching the new product or service.

4.3.4 Proposals to introduce new products or services should generally include:

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

- a detailed risk assessment, including whether the new product or service is within the AI's risk appetite, implications for the AI's risk profile (for example, in terms of credit, market, interest 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);

- a cost and benefit analysis;
- 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);
- an analysis of the proposed scale of new activities in relation to the AI's overall financial condition, including its capital strength and liquidity resources; and
- the procedures to be used for measuring, monitoring, controlling or mitigating, and reporting the risks.

4.3.5 All relevant functions, e.g. risk management, accounting, operations, legal and compliance, information technology should be consulted (for instance through a new product committee established within the AI), before a new product or service is launched. Such functions should 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 should escalate and report to the Board (or its designated committee(s)) if there is any significant concern (e.g. material impact on the AI's risk profile) with regard to any new product or service before its launch.

4.3.6 AIs should perform a comprehensive post-implementation evaluation of new products or services (as well as existing products or services following any significant changes to their features or risk profile) to ensure no risk remains unidentified or unaddressed. The evaluation results should be taken into account for the development of any similar products or services in the future. In addition, AIs should perform regular reviews of products and services (adopting a risk-based approach as appropriate).

4.3.7 The Chief Risk Officer should have a holistic oversight of the risks to the AI associated with new products and services and the related risk management processes. To

achieve this, the risk management function should monitor and participate in the process of approving new products or services (or significant changes to existing products or services), and should maintain a centralised list of approved products and services[8]. 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 should also be responsible for determining whether a new initiative should 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 AI's formal approval process applicable to new products or services.

4.3.8 The internal audit function should 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.

5. Risk management systems and processes

5.1 Risk management function

Key responsibilities and attributes

5.1.1 AIs should establish a dedicated risk management function to carry out day-to-day risk management activities across the whole organisation.

5.1.2 An effective risk management function should:

- have clearly defined responsibilities and accountability;

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

- have a direct reporting line to senior management and direct access to the Board or its Risk Committee (see also paragraph 5.1.6 below);

- 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;

- be supported by an effective management information system; and

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

5.1.3 The responsibilities of an AI's risk management function include:

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

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

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

- 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 AI'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 AI as a whole;

- 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;

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

- providing accurate, reliable and comprehensible 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

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

Chief Risk Officer

5.1.4 AIs are expected to appoint a person to be responsible for the risk management function, commonly known as the Chief Risk Officer, who should also coordinate the risk management activities of other units within the organisation. It is generally expected that the Chief Risk Officer will be part of the senior management team, and his appointment (or cessation of appointment) will be

approved by the Board (or its designated committee) and publicly disclosed. In exceptional cases where, for example, an AI'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 AI.

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

5.1.6 The Chief Risk Officer should have a direct reporting line to the AI's Chief Executive and should 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 should play a key role in enabling the Board, Risk Committee and senior management to understand the AI's evolving risk profile against the approved risk appetite, and should report to the Board and the Risk Committee promptly on any material breach of risk limits and any adverse development that may result in the AI's risk appetite being exceeded. The performance and remuneration of the Chief Risk Officer should be reviewed and approved by the Board (or its designated committee).

5.1.7 As part of his responsibilities for the AI's risk management function, among other things, the Chief Risk Officer should ensure that prompt action is taken when any material risk exposure is close to, or exceeds, the AI's approved risk appetite and relevant risk limits.

Furthermore, the Chief Risk Officer should participate in key decision-making processes (e.g. strategic planning, capital and liquidity planning, new products and services approvals, remuneration design and operation) and should be involved in the setting of risk-related performance indicators for business units.

5.2 Risk management information system[9]

5.2.1 An AI should 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.

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

- 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 should be able to generate any necessary data rapidly in times of stress;

- capturing, aggregating and reporting risk data on all sources of relevant risks on a range of bases,

---

[9] This section serves to provide some general guidance for application to all AIs (albeit on a proportionate basis), having regard to the *"Principles for effective risk data aggregation and risk reporting"* issued by the Basel Committee on Banking Supervision in January 2013. A higher standard is expected of any AI which is designated by the Monetary Authority as a global systemically important bank pursuant to section 3S of the BCR or a domestic systemically important bank pursuant to section 3U of the BCR. Such an AI should 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.

including by business line, product, portfolio, function, and at entity and group levels;

- supporting customised identification, aggregation and reporting of risks (e.g. based on individual or a set of closely related risk drivers) to meet requests of the Board, senior management and other users, including the HKMA;

- incorporating changes arising from regulatory requirements and new business developments as and when necessary;

- supporting a broad range of risk management analysis, including but not limited to:

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

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

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

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

  - conducting variance analysis against annual budget or business targets, and calculating risk-adjusted performance (see subsection 5.4 below);

  - providing adequate system support for fair valuing exposures; and

  - conducting sensitivity analysis and stress-testing (see subsection 5.5 below), and generating

forward-looking firm-wide scenario analyses on evolving market conditions and stressed conditions.

5.2.3 Risk management reports should 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 should be appropriate for the needs of recipients. While individual AIs should determine risk reporting requirements that are appropriate for their own business models and risk profiles, at a minimum, the reports should cover all material risk areas (e.g. credit, market, interest 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 should provide information relating to regulatory ratios (e.g. capital adequacy ratios and liquidity ratios) and their projections.

5.2.4 There should be proper control, validation and reconciliation processes in place to ensure the accuracy of risk management reports, and relevant processes should be documented with appropriate explanation. For instance, it is expected that risk data aggregation should occur on a largely automated basis. There should be automated and manual checks, including validation rules to help verify data inputs and calculations. Risk data and reports should be reconciled with other relevant sources (e.g. accounting data and reports) where appropriate. The risk management reports should 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).

5.2.5 To remain effective, there should be processes to identify, rectify and alert the senior management (where appropriate) of any incompleteness, exception, limitation

and weakness of the AI's risk management information system in capturing, aggregating and reporting of risks. The system should also be subject to regular review and enhancement. Moreover, the capabilities of the AI's risk management system should 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 should be set for making any required upgrading or adjustment.

5.3 Risk measurement and assessment

5.3.1 AIs should 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).

5.3.2 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, an AI should, among other things, consider the following factors:

- the nature, scale and complexity of its business activities;
- its business needs (e.g. for pricing);
- the assumptions underpinning the methods or models;
- data availability;
- the sophistication of its management information system; and
- staff expertise.

5.3.3 The Board or its designated committee(s) and senior management should 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 should also satisfy themselves as to the adequacy and appropriateness of the key assumptions, data sources and procedures used to measure or assess the risks.

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

5.3.5 AIs should avoid over reliance on any specific risk methodology or model. Modelling and risk management techniques should 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, AIs should use a range of risk measures or tools to provide different views of risk on the same exposures.

5.3.6 Similarly, decisions which determine the level of risks to be taken should not only be based on quantitative information or model outputs, but should also take into account 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 should explicitly be addressed to identify their potential impact on particular business activities. Such assessments should be formally integrated into material risk decisions.

5.3.7 AIs should 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, AIs should 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.

5.3.8 For risk measurement purposes, AIs should be able to value their positions (including those associated with complex products and financial instruments) based on sound valuation practices. This should be the case both in normal times and in times of stress. For exposures that represent material risk, AIs should 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.

5.4 Risk-adjusted performance measurement

5.4.1 AIs are expected to adopt a system for measuring the performance of their business units on a risk-adjusted basis to enable them to compare the financial performance of individual business units, taking into account 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.

5.4.2 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 AIs should be able to comprehensively measure the risks associated with the units' business activities. Management information systems should 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).

5.4.3 Data inputs and information used for the purpose of calculating remuneration payable to an AI's senior

management and staff should be subject to independent review to ensure their appropriateness and accuracy.

5.5 Sensitivity analysis and stress-testing

5.5.1 AIs should have adequate systems and capability to measure the sensitivity of earnings to a change in individual risk factors (e.g. interest rates) and conduct stress tests to:

- identify possible events or market changes that could have serious adverse effects or a significant impact on their overall risk profiles and financial positions;
- address existing or potential risk concentrations; and
- facilitate the development of risk mitigating measures or contingency plans across a range of stressed conditions.

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

5.5.3 The Board (or its Risk Committee) and senior management should 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 should be taken into account in the setting of policies and limits.

5.5.4 See IC-5 “Stress-testing” for more guidance on the use of stress tests for risk management purposes.

6. Internal controls, audits, contingency planning and reporting and notification requirements~~Internal controls, audits and contingency planning~~

6.1 Internal control system

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

6.1.2 A properly structured internal control system should:

- help to promote effective and efficient operation;
- provide reliable financial information;
- safeguard assets;
- minimise the operating risk of loss from irregularities, fraud and errors;
- ensure effective risk management systems; and
- ensure compliance with relevant laws, regulations and internal policies.

6.1.3 An AI's internal control system should, at a minimum, cover the following:

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

- controls relating to information technology (see TM-G-1 "General Principles for Technology Risk Management");

- controls relating to outsourced activities, where applicable (see SA-2 "Outsourcing"); and

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

6.1.4 An effective internal control system requires a strong control environment[10] to which the Board and senior management provide their full support, and an internal audit function to evaluate its performance on a regular basis (see subsection 6.2 below).

6.2 Internal audit function

6.2.1 AIs' internal audit function (see also IC-2 "Internal Audit Function") should, 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.

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

6.2.3 In fulfilling its responsibilities relating to an AI's risk management, the internal audit function should, among other things, assess (on a group basis and on the basis of individual business units and legal entities) and report

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

to the Board (or its Audit Committee) periodically whether:

- the AI's risk governance arrangements and risk appetite framework are effective, both in their design and operation (including the linkages to the AI's risk culture, strategic and business planning, remuneration and decision-making processes);
- breaches of risk limits are being appropriately identified, escalated and reported;
- the AI's risk measurement techniques and risk management information system and related reporting are effective; and
- the AI's internal control system is effective.

6.2.4 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 should be directly and promptly reported to the Board (or its Audit Committee) and senior management for early rectification.

6.2.5 An AI should 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.

6.3 Compliance function

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

6.3.2 The primary role of an AI's compliance function is to assist the AI 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 AI 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 an AI have their respective responsibility for ensuring compliance.)[11]

6.3.3 Key responsibilities of the compliance function include[12]:

- identifying, assessing and monitoring compliance risk;
- advising senior management on the laws, rules and standards (and any changes of such) with which the AI is required to comply;
- establishing the AI's compliance policies and guidelines, and ensuring that they remain effective;
- providing compliance-related advice and training to staff;
- reporting regularly to, and advising senior management on, compliance matters; and
- establishing a compliance programme that sets out its planned activities, including the scope of review of policies and procedures to ensure the AI's compliance with applicable statutory provisions, regulatory requirements and codes of conduct.

6.3.4 An AI is expected to have an independent compliance function and to appoint a person (commonly known as

---

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

[12] 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 should be clear.

the Head of Compliance) to be responsible for the firm-wide compliance function or, in the case of an ~~overseas-incorporated~~ AI incorporated outside Hong Kong, the compliance function of its Hong Kong branch. The appointment of the Head of Compliance should be approved by the Board (or its designated committee). An AI should promptly and in any event within 14 days, notify the HKMA of the appointment (and cessation of appointment) of its Head of Compliance.[13]

6.3.5 In exceptional cases where, for example, an AI's scale of operations may not justify having all necessary tasks carried out internally by the compliance function, other arrangements (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 should nevertheless be adequate oversight by the AI's Head of Compliance.

6.3.6 An effective compliance function should:

- have adequate resources and be staffed by an appropriate number of competent staff who are sufficiently independent of the business and operating units. The Head of Compliance and the staff of the compliance function should 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; [14]

- be given appropriate standing and authority within the AI. It should report to a designated committee of the Board (e.g. the Audit Committee) or senior

[13] This notification requirement is applicable irrespective of whether the person appointed as the Head of Compliance is a "manager" as defined in section 2 of the ~~Banking Ordinance~~BO.

[14] For instance, among other things, the Head of Compliance should not have responsibilities for any business units of the AI. Remuneration of the Head of Compliance and staff of the compliance function should not be influenced by, or linked to the performance of, the business and operational units which are subject to monitoring by the compliance function.

management and have the right to report matters to the Board directly as necessary; and

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

6.3.7 To ensure effective management of compliance risk, the AI's compliance policy should document the organisation, status and responsibilities of the compliance function as well as other measures to manage compliance risk. The Board should approve the policy and should 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) should have the required independence to take up the mandate. The Board should monitor the committee's performance to ensure that its directives are properly followed.[15]

6.4 Contingency, business continuity and recovery planning

6.4.1 Each AI should, as part of its business continuity planning, contingency funding planning and recovery planning, ensure that the AI's risk management function will be able to fulfil its roles and responsibilities effectively in emergency and crisis situations.

6.5 Reporting and notification requirements

[15] In the case of an ~~foreign bank~~ AI incorporated outside Hong Kong operating a branch in Hong Kong, the head office of the ~~bank~~ AI may authorize 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.

6.5.1 A number of provisions of the BO and various rules made under the BO require an AI to report, or notify the HKMA of, certain matters. In addition, an AI is expected to report, or notify the HKMA of, other matters which are specified in various SPM modules or through other means of regulatory communication. An AI should have adequate systems, controls and processes, underpinned by robust governance framework, to ensure that matters required to be notified or reported to the HKMA are identified in a timely manner and notified or reported to the HKMA as required.

6.5.2 An example of such notification and reporting requirements is that pursuant to section 67(1) of the BO, an AI must, **immediately on becoming aware** of any material adverse development that has occurred, or is likely to occur, in relation to the institution: (i) give written notice to the MA, and (ii) submit a report of all relevant facts, circumstances and information to the MA together with the notice.

6.5.3 While the expression "material adverse development" is not defined, section 67(2) of the BO provides (without limiting the meaning of the expression) that a material adverse development occurs if:

- the development is one that has, or is likely to have, an adverse effect on (i) the financial soundness or viability of the institution or (ii) the ability of the institution to continue to carry on its banking business or business of taking deposits; or

- the institution is likely to become unable to meet its obligations or is about to suspend payment.

6.5.4 Since the meaning of "material adverse development" is not confined by section 67(2) of the BO, an AI should put in place processes that enable it not only to promptly identify the developments specified in section 67(2) but also to promptly assess whether other developments that occur, or are likely to occur, in relation to the institution are material adverse developments and hence to be notified immediately to the MA together with a report of

all relevant facts, circumstances and information. As each situation is fact-specific, it is not practicable to set out in this module all potential notifiable developments or to provide any specific material threshold in a definitive manner for the purpose of section 67. However, by way of guidance, the following are examples of the sort of developments that the HKMA would generally expect to be notified and reported under section 67:

- a matter involving a financial loss (e.g. credit-related or otherwise) incurred or to be incurred by an AI that has or is likely to have a material adverse impact on the AI's financial position (such as in terms of capital adequacy, liquidity, profit and loss etc);

- an operational incident (including an IT incident) that causes, or is likely to cause, prolonged or severe disruption to an AI's operations and/or services to customers, or that has, or is likely to have, a material adverse impact on a significant number of customers;

- a non-financial incident (e.g. fraud, legal or regulatory action against an AI, or a breach of legal or regulatory requirement) that poses, or is likely to pose, material adverse reputation, financial or other risks to the institution;

- a development relating to an AI's group of companies that poses, or is likely to pose, material adverse financial or non-financial risks to the AI; or

- a development that renders, or is likely to render, an AI unable to meet the minimum criteria for authorization (as provided in the Seventh Schedule to the BO) on a continuing basis.

Annex 1

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 AIs themselves
- 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 arrangement (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)