HONG KONG MONETARY AUTHORITY 香港金融管理局		
Supervisory Policy Manual		
IC-1	**General Risk Management Controls**	V.2 – 31.12.2010

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 general controls which the MA expects AIs to have in place in their risk management systems

Classification

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

Previous guidelines superseded

IC-1 "General Risk Management Controls" (V.1) dated 25.04.03

Application

To all AIs

Structure

1. Introduction
   - 1.1 Background
   - 1.2 Scope and overview
2. Board and senior management oversight
   - 2.1 Risk management role and governance
   - 2.2 Setting of risk appetite
   - 2.3 Firm-wide risk management
   - 2.4 Use of specialised committees
3. Risk management policies, procedures and limits

3.1 Policies and procedures
3.2 Risk limits
3.3 New products and services
4. Risk management systems and processes
4.1 Risk management function
4.2 Risk management information system
4.3 Risk measurement and assessment systems
4.4 Risk-adjusted performance measurement
4.5 Sensitivity analysis and stress-testing
5. Internal controls, audits and contingency planning
5.1 Internal control system
5.2 Internal audit function
5.3 Compliance function
5.4 Contingency and business continuity planning

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 system that is commensurate with the size and complexity of an AI's operations needs to be in place to help ensure that the risks undertaken are well managed within the AI's risk appetite and that the system achieves its intended results.

1.1.2 According to the "Core Principles for Effective Banking Supervision" issued by the Basel Committee in October 2006, banking supervisors should be satisfied that banks have in place a comprehensive risk management process (including Board and senior management oversight) to identify, measure, monitor and control or mitigate all material risks and to assess their overall capital adequacy in relation to their risk profile.

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 section 2 of SA-1 "Risk-based Supervisory Approach"). Locally incorporated AIs 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 For the purposes of this module, "risk management" refers broadly to the policies, systems and procedures adopted by AIs in identifying, measuring, monitoring, controlling or mitigating, and reporting the various types of risk they face.

1.2 Scope and overview

1.2.1 This module is intended to cover general systems and controls relating to risk management. Some of the specific systems and controls associated with various inherent risks specified in para. 1.1.3 above are separately described in the relevant modules, including:

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

1.2.2 In addition, this module stresses the importance of each AI having a sound firm-wide risk management framework that enables the AI to set its appetite and tolerance for risks, and supports the Board and senior management in managing its risks from an integrated, firm-wide perspective and in identifying and reacting to emerging and growing risks in a timely and effective manner.[3]

---

1 The module is under development.

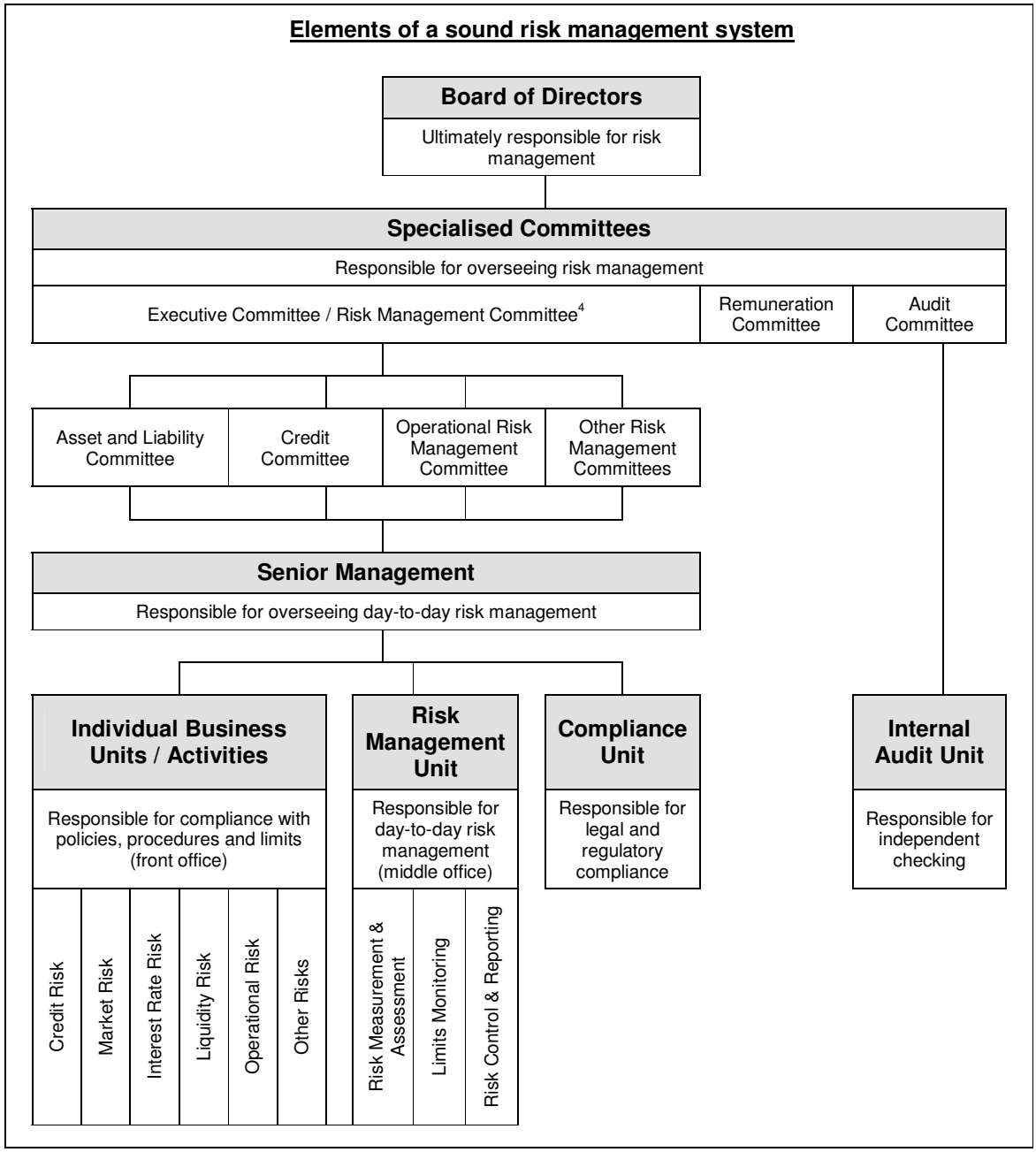
2 The module is under industry consultation.

3 For a banking group, the concept of firm-wide risk management will similarly apply on a group-wide basis, i.e. through managing the relevant risks of the parent bank and its group entities as a whole.

1.2.3 While risk management systems may vary among AIs, the basic elements contributing to a sound risk management environment are:

- appropriate Board and senior management oversight (see section 2 below);
- adequate organisational policies, procedures and limits to identify and manage all relevant risks across business activities (see section 3 below);
- adequate risk measurement, monitoring and reporting systems to support all business activities and related risks (see section 4 below);
- well-established internal controls and comprehensive audits to detect any deficiencies in the internal control environment in a timely fashion (see section 5 below); and
- sufficient arrangements to deal with contingency or emergency situations (see section 5 below).

1.2.4 An overview of how the elements above fit together is illustrated below. This illustration is not intended to be prescriptive but is indicative of the elements of a sound risk management system.



[4] In some cases, a Risk Management Committee is established specifically to take up the function of overseeing the various aspects of risk management on an integrated basis.

1.2.5 The standards laid down in this module will be applied to AIs on a proportionate basis, having regard to their size, nature and complexity of operations. AIs will also be expected to apply similar risk management systems and processes to their subsidiaries and, to the extent practicable, associated companies and joint ventures which may expose them to significant potential risk[5].

1.2.6 Failure to adhere to the general requirements set out in this module may call into question whether an AI continues to satisfy the minimum criteria for authorization in the Banking Ordinance and cast doubt on the fitness and propriety of its directors, chief executives and senior management.

2. Board and senior management oversight

2.1 Risk management role and governance

2.1.1 The Board and senior management of an AI have the primary responsibility to understand the risks run by the AI and ensure that these risks are properly managed.

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

- have knowledge and expertise sufficient 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;

[5] 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.

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

- 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;

- maintain continued awareness of the AI's business profile and risks as well as 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;

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

- 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; and

- 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").

2.1.3 In order to ensure sound risk governance, the Board and senior management should establish a comprehensive and independent risk management function[6] to monitor and

[6] Some AIs may refer to this function as the "risk control function".

coordinate risk management activities across the entire organisation (see subsection 4.1 below).

2.1.4 The Board and senior management should also promote the establishment of regular and transparent communication mechanisms within the organisation, so that there is continuous and robust dialogue and information sharing among members of senior management[7], business line risk owners, and independent risk management and control functions in respect of firm-wide risk measurement, analysis and management issues. Consideration should be given to forming a Risk Management Committee for this purpose.

2.1.5 Risk governance arrangements (including responsibilities, structure, risk appetite, etc.) should be documented and updated as appropriate. All relevant staff (including business units) should be informed of these arrangements and their respective roles in the oversight and management of risk.

2.2 Setting of risk appetite

2.2.1 An AI's risk appetite (or risk tolerance) describes the level of risk the AI is willing to take, having regard to its financial capacity, strategic direction and regulatory constraints (e.g. capital and liquidity requirements).

2.2.2 The Board is responsible for setting the overall risk appetite of the AI and approving its risk appetite statements. While there is no common way of expressing risk appetite, an AI's risk appetite statements should be comprehensive, include appropriate risk targets[8] that are consistent with one other, and reflect a suitably wide range of measures and actionable elements that clearly articulate the AI's intended responses to a range of possible events, e.g. a loss of capital or a breach in risk limits. Management actions documented in the statements should be realistic and

[7] These include the Chief Executive, the Chief Risk Officer and other members at that level.

[8] Examples of risk targets include target credit ratings and target rates of return on equity.

feasible for restoring capital or reducing risk in adverse situations.

2.2.3 In setting the risk appetite, the Board should ensure that all relevant risks of the AI are taken into account, including those that are less quantifiable (e.g. reputation risk) or arise from off-balance sheet transactions. The AI should be able to express its overall risk appetite in a manner that is suitable for the nature and complexity of its business. This process may involve, for example, assessing both the financial and non-financial implications of all relevant risks (through quantitative analysis, stress-testing, reference to historical experience, exercise of judgement or otherwise), setting individual risk limits for more quantifiable risks and determining an overall cap to govern the aggregate level of risk exposures that the AI is willing to assume.

2.2.4 The Board should be satisfied that robust procedures and controls are in place for setting and monitoring the AI's risk appetite. Sufficient information should be compiled to facilitate regular assessment of the risk appetite by the Board and senior management, 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.

2.2.5 When faced with 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's direction is critical to sustaining a disciplined risk appetite for the AI. In these circumstances, the Board should adopt a prudent approach, and should thoroughly understand the AI's current risk position relative to its risk appetite and how the position would be changed if the risk appetite was changed. In this regard, stress tests may be used to generate a dynamic view of the AI's capital and risk positions.

2.2.6 The Board should approve any changes to the AI's risk appetite statements. The justification for change should be adequately documented.

2.3 Firm-wide risk management

2.3.1 The Board and senior management should ensure that an effective risk management framework is in place to facilitate an integrated approach to managing the AI's firm-wide risks (e.g. credit, market and other major risks).

2.3.2 This framework should enable the identification and management of all major risks across business activities, whatever the nature of the exposure (which may be non-contractual, contingent or off-balance sheet in nature).

Specific responsibilities of the Board

2.3.3 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;
- 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 3.3 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 the information systems and infrastructure 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

2.3.4 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 and all levels of staff should 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 business or risk management functions, with appropriate programmes to recruit, train and retain employees with suitable skills and expertise.

2.4 Use of specialised committees

2.4.1 While the Board is ultimately responsible for risk management, it may delegate authority to one or more than one specialised committee such as a Credit Committee or Asset and Liability Committee (see also section 4 of CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions") to carry out some of the functions described in para. 2.3.3 above. Delegation of authority should be made on a formal basis, e.g. with a clear mandate. Appropriate reports should be submitted regularly to the Board by the committee or committees to which such authority has been delegated.

2.4.2 Such delegation of authority, however, 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. Moreover, individual members of the Board will still be 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. limits), used to manage the risks.[9] If existing members lack the relevant expertise, bringing in new members with such knowledge or appointing external consultants should be considered.

[9] For example, some members should preferably have had practical experience in financial markets or have obtained, from their business activities, sufficient professional experience directly linked to such type of activity.

3. Risk management policies, procedures and limits

3.1 Policies and procedures

3.1.1 AIs should have clearly defined policies and procedures that enable firm-wide risks to be managed in a proactive manner[10], 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.

These documents should be approved by the Board or its designated committee(s).

3.1.2 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.

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

- an AI's overall business strategy and activities;
- the appropriateness to the size, nature and complexity of the AI's business activities;
- the risk appetite of the AI;

[10] Overseas incorporated AIs 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 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.

3.1.4 Accountability and the lines of authority for each business line or unit, should be spelled out clearly in the policies and procedures, and updated as appropriate.

3.1.5 The risk management policies and procedures should keep pace with the changing environment. The Board or its designated committee(s) should review these documents on a regular basis (e.g. at least annually). If the review is carried out by the committee(s) or senior management, any material amendment to the policies and procedures should be submitted to the Board for adoption and formal ratification.

3.1.6 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.

3.2 Risk limits

3.2.1 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).

3.2.2 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.

3.2.3 Risk limits should be suitable to the size and complexity of an AI's business activities and compatible with the sophistication of its products and services. 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.

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

3.2.5 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.

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

3.2.7 Limit utilisation should be closely monitored. Any excesses or exceptions should be reported promptly to senior management for necessary action.

3.3 New products and services

3.3.1 AIs should have in place an internally approved and well-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 of existing products and services. The approach to determining whether changes to existing products and services are considered to be "significant" should also be documented.

3.3.2 The new product approval policy of an AI should, at a minimum, cover the following areas:

- all aspects of the decision to enter new markets or 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 involved in the decision (either through a standing or ad hoc committee);
- 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.

3.3.3 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 financial resources to launch the product or service, as well as adequate internal tools and expertise to monitor the risks associated with it.

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

- a description of the new product or service;
- a detailed risk assessment;
- 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. system enhancement);
- an analysis of the proposed scale of new activities in relation to the AI's overall financial condition and capital strength; and
- the procedures to be used for measuring, monitoring, controlling or mitigating, and reporting the risks.

3.3.5 All relevant departments, e.g. risk control, accounting, operations, legal and compliance, should be consulted as appropriate, before a new product or service is launched. New products or services which could have a significant impact on an AI's risk profile should be brought to the attention of the Board or its designated committee(s) before the launch.

3.3.6 AIs should perform a post-implementation evaluation of new products or services, the results of which should be taken into account for the development of any similar products or services in the future.

3.3.7 The risk management function should participate in the process of approving new products or services (or significant changes to existing products or services). It should also have a clear overview of the roll-out of new products or services (or significant changes to existing products or services) across different business activities. Where appropriate, it should have the power to require that significant changes to existing products or services go through the formal approval process applicable to new products or services.

4. Risk management systems and processes

4.1 Risk management function

Key responsibilities and attributes

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

4.1.2 An effective risk management function should:

- have clearly defined responsibilities;
- have a direct reporting line to the relevant Risk Management Committee or senior management;
- 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 (see subsection 4.2 below); and
- be given adequate authority, management support and resources to perform its duties, and be staffed by persons with the relevant expertise and knowledge.

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

- ensuring that all relevant risks of the AI are identified, well understood, and adequately measured and assessed;
- ensuring that the AI's risk management framework, and all related policies and control procedures, are adequately implemented and complied with;
- 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 the use of risk limits and ensuring that quantifiable risks are within the structure of approved limits. 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 exceptional transactions;
- ensuring that all relevant risks of the AI are properly measured and controlled, and all identified risk management issues or concerns are promptly reported to the Board and the relevant Risk Management Committee or senior management; and
- alerting the Board and the relevant Risk Management Committee or 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

4.1.4 AIs are expected to appoint a person to be responsible for the risk management function (commonly known as the Chief Risk Officer), who will also coordinate the risk management activities of other units within the organisation. 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 executives (such as the person in charge of internal control) may share this responsibility.

4.1.5 The Chief Risk Officer (or equivalent) should have sufficient independence and seniority to enable him to challenge an AI's decision-making process. He should be able to communicate directly with senior management and, where appropriate, report to the Board or its designated committee(s), about adverse developments that may not be consistent with the AI's risk appetite and business strategy.

4.1.6 The Chief Risk Officer (or equivalent) should have skills and experience which are relevant and appropriate to the nature and complexity of an AI's business activities, and should play a key role in enabling the Board and senior management to understand the AI's overall risk profile.

4.2 Risk management information system

4.2.1 AIs should establish and maintain a management information system with adequate technological support and processing capacity (even in times of stress) to effectively measure and report on the risks of major business activities within the organisation.

4.2.2 An effective risk management information system should produce timely, accurate and reliable reports for the Board, senior management and line managers to support decision-making at the different levels, and to enable early identification of emerging risks.

4.2.3 The level of sophistication of the system should depend on the nature, scale and complexity of an AI's business activities. Generally, it should be capable of:

- measuring the risks of a product or an activity in accordance with the measurement methods or models adopted;
- aggregating data on a product, functional, geographical and group basis and, to the extent necessary, all sources of relevant risks by business line, portfolio and entity;
- supporting customised identification and aggregation of risk concentrations within the AI (based on individual, or a set of closely related, risk drivers);
- 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;
- producing information at appropriate intervals. In times of stress, the system should be capable of generating reports at more frequent intervals as required by management;
- 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 4.4 below);
- providing adequate system support for fair valuing exposures; and

- conducting sensitivity analysis and stress-testing (see subsection 4.5 below).

4.2.4 To enable proactive risk management, the system should be adaptable and responsive to changes in the assumptions used for risk measurement and aggregation, be capable of incorporating multiple perspectives of risk exposure to account for uncertainties in risk measurement, and be sufficiently flexible to allow for generation of forward-looking firm-wide scenario analyses that capture management's interpretation of evolving market conditions and stressed conditions.

4.2.5 If AIs use third-party inputs or other tools (e.g. credit ratings, risk measures and models, etc.) to produce risk management information, they should have adequate procedures in place to ensure that such inputs and tools are subject to initial and ongoing validation.

4.2.6 To remain effective, the system should be subject to regular upgrade and modification.

4.3 Risk measurement and assessment systems

4.3.1 AIs should have in place effective systems 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).

4.3.2 Different methods or models may be used to assess or measure each type of risk. For example, a number of value-at-risk ("VaR") approaches such as historical simulation, variance/co-variance method or Monte Carlo simulation can be used to estimate the exposure of an AI to various types of market risk. An AI may also choose to use a risk mapping process[11], key risk indicators or scorecards as a means of assessing its operational risk. Detailed

[11] In this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.

guidance on the measurement or assessment of individual risks can be found in the relevant modules listed in para. 1.2.1 above.

4.3.3 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 of the methods or models;
- data availability;
- the sophistication of its management information system; and
- staff expertise.

4.3.4 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.

4.3.5 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.

4.3.6 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.

4.3.7 Similarly, decisions which determine the level of risks 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 in material risk decisions.

4.3.8 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 (e.g. VaR) 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.

4.3.9 For risk measurement purposes, AIs should be able to value their positions (including those associated with complex products and financial instruments), especially in times of stress, based on sound valuation practices. 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 not relevant due to market disruptions or

illiquidity. See CA-S-9 "Financial Instrument Fair Value Practices" for more details.[12]

4.4 Risk-adjusted performance measurement

4.4.1 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. This ensures that business units are not rewarded for taking on excessive risks.

4.4.2 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 their 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).

4.4.3 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.

4.5 Sensitivity analysis and stress-testing

4.5.1 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;

[12] This module is under industry consultation.

- address existing or potential risk concentrations; and
- facilitate the development of risk mitigating measures or contingency plans across a range of stressed conditions.

4.5.2 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 activities.

4.5.3 The Board 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.

4.5.4 See IC-5 "Stress-testing" for more guidance on the use of stress tests for risk management purposes.

5. Internal controls, audits and contingency planning

5.1 Internal control system

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

5.1.2 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.

5.1.3 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");
- controls relating to compliance with statutory and regulatory requirements (see subsection 5.3 below); and
- controls relating to the prevention of money laundering (see Guideline on Prevention of Money Laundering,

Supplement to the Guideline, and interpretative notes issued in July 2010).

5.1.4 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 its performance on a regular basis (see subsection 5.2 below).

5.2 Internal audit function

5.2.1 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.

5.2.2 The risk management process and related internal controls should be examined 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.

5.2.3 To carry out their function effectively, internal auditors should:

- preserve objectivity and impartiality by avoiding any conflict of interest in performing their duties;
- have unfettered power to choose which business or operating units to be audited and to access records and documents;
- have appropriate independence and status within the AI to ensure that senior management reacts to, and acts upon, their recommendations;

[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.

- have sufficient resources, be suitably trained, and possess relevant expertise and experience to understand the risk management process and measurement models or methods employed; and

- employ a methodology that identifies the key risks run by the AI and allocates their resources accordingly.

5.2.4 All identified risk management deficiencies and weaknesses (including any non-compliance with internal policies and procedures as well as stipulated regulatory requirements on risk management) should be directly and promptly reported to the Board (or the Audit Committee) and senior management for early rectification.

5.3 Compliance function

5.3.1 The compliance function plays an important role with respect to a sound risk management system, but should not be considered as a substitute for regular and frequent internal audit coverage.

5.3.2 The primary role of an AI's compliance function is to ensure that the AI is in compliance with the statutory provisions, regulatory requirements and codes of conduct applicable to its banking or other regulated activities[14].

5.3.3 Other responsibilities of the compliance function include[15]:

- identifying, measuring and assessing compliance risk;

- advising senior management on the laws, rules and standards with which an AI is required to comply;

---

[14] 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 Department, responsible for providing advice on, or monitoring the legal implications associated with, such areas.

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

- providing compliance-related guidance and training to staff;

- monitoring and testing compliance, and reporting regularly to senior management on compliance matters; and

- establishing a compliance programme that sets out its planned activities.

5.3.4 AIs are expected to have a separate, independent compliance function. In exceptional cases where, for example, an AI's scale of operations may not justify having such a function, other arrangements (such as hiring an external lawyer to provide legal advice on a need basis or an appropriate allocation of duties among departments) may be acceptable.

5.3.5 An effective compliance function should:

- be staffed by an appropriate number of competent staff who are sufficiently independent of the business and operating units;

- be given appropriate standing and authority within an AI, with a direct reporting line to a designated committee (e.g. Audit Committee) or senior management; 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.

5.3.6 In addition, compliance staff, in particular the Head of Compliance, 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.

5.3.7 To ensure effective management of compliance risk, the Board should approve the AI's compliance policy, which should document the organisation, status and responsibilities of the compliance function as well as other measures to manage compliance risk, and 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 direct an appropriate board level committee (e.g. the Audit Committee) to establish the compliance policy and conduct regular review of how the policy has been implemented. In such a case, the Board should monitor the committee's performance to ensure that its directives are properly followed.[16]

5.4 Contingency and business continuity planning

5.4.1 Each AI should have in place contingency and business continuity plans, having regard to the nature, scale and complexity of its business activities, to ensure that it has adequate arrangements to deal with emergency or crisis situations (see LM-2 "Sound Systems and Controls for Liquidity Risk Management" and RR-1 "Reputation Risk Management") and can continue to function and meet its regulatory obligations in the event of an unforeseen interruption (see TM-G-2 "Business Continuity Planning"). These plans should be regularly updated and tested to ensure their effectiveness.

Contents | Glossary | Home | Introduction

[16] In the case of a foreign bank operating a branch in Hong Kong, the head office of the bank may authorize the branch to establish the compliance policy for the local operations, provided that the completed 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.