HONG KONG MONETARY AUTHORITY
香港金融管理局

Supervisory Policy Manual

OR-1	Operational Risk Management	V.1 – 28.11.05

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 set out the approach which the HKMA will adopt in the supervision of AIs' operational risk, and to provide guidance to AIs on the key elements of effective operational risk management

Classification

A non-statutory guideline issued by the MA as a guidance note

Previous guidelines superseded

This is a new guideline.

Application

To all AIs

Structure

4. Organisational structure
   - 4.1 Overview
   - 4.2 Board oversight
   - 4.3 Senior management responsibilities
   - 4.4 An operational risk management function
   - 4.5 Roles of business line management
   - 4.6 Other operational risk related functions
   - 4.7 Role of internal audit
5. Risk culture
6. Operational risk management strategy, policies and procedures
   - 6.1 Strategy
   - 6.2 Policies
   - 6.3 Definition of operational risk
7. Operational risk management process
   - 7.1 Overview
   - 7.2 Risk identification and assessment
   - 7.3 Risk monitoring and reporting
   - 7.4 Risk control and mitigation
8. Business continuity management and disaster recovery plan

1. Introduction

1.1 Background

1.1.1 As set out in the HKMA's risk-based supervisory approach under section 2 of SA-1 "Risk-based Supervisory Approach", AIs are generally subject to eight major types of risks - credit, market, interest rate, liquidity, operational, reputation, legal and strategic. They are expected to establish a sound and effective system to manage each of these risks.

1.1.2 Operational risk is present in virtually all bank transactions and activities. It is defined by the Basel Committee under its revised framework on capital standards for banks ("Basel II") as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition includes legal risk but excludes strategic and reputational risk.

1.1.3 Operational risk has become an increasing issue over the last few years as banks:

- rely more on increasingly complex automated technology;
- develop more complex products;
- are involved in large scale mergers and acquisitions;
- initiate consolidation and internal reorganisation;
- adopt techniques which are devised to mitigate other forms of risks (e.g. collateralisation, credit derivatives, netting and asset securitisation), but potentially create other forms of risk (e.g. legal risk); and
- outsource some of their functions.

Failure to implement proper processes and procedures to control operational risks has resulted in significant operational losses for some banks in recent years.

1.1.4 In February 2003, the Basel Committee issued a paper entitled "Sound Practices for the Management and Supervision of Operational Risk" for use by banks and

supervisory authorities when evaluating operational risk management policies and practices. The Basel Committee believes that the principles outlined in the Paper establish sound practices relevant to banks of any size and scope. Therefore, it recommends compliance with its guidance set out in the Paper for all approaches to measuring an operational risk capital charge under Basel II. It also requires that use of the more advanced measurement approaches i.e. the Standardized (Operational Risk) Approach (STO Approach) (and Alternative Standardized Approach (ASA Approach)) or the Advanced Measurement Approaches (AMA Approach) be conditional upon the fulfilment of specific operational risk management criteria.

1.2 Scope

1.2.1 This module:

- sets out the HKMA's supervisory approach to operational risk;
- provides guidance on the key elements of a sound operational risk management framework; and
- provides additional guidance on how the qualitative criteria for using the STO Approach (or ASA Approach) to calculate operational risk capital charge under Basel II may be met by AIs.

1.2.2 In developing this module, the HKMA has made reference to:

- the Paper issued by the Basel Committee as mentioned under para. 1.1.4 above;
- the qualifying criteria for adopting the STO Approach (or ASA Approach) to calculate operational risk capital charge under Basel II;
- the operational risk management policies and practices adopted by some international banks; and
- Principle 13 of the "Core Principles for Effective Banking Supervision" covering banks' risk management processes for controlling other material risks (including operational risk) (the relevant information is contained in the Basel

Committee paper on "Core Principles Methodology" (1999)).

1.2.3 For the purpose of this guidance, there is no standard measure of materiality, criticality or significance of an operational event or exposure as it varies among AIs. In determining the relative significance of an operational event or exposure, AIs may take into account both qualitative and quantitative factors that are relevant to their own circumstances and assess both the current and future impact of such factors on their capital, earnings, franchise or reputation.

1.3 Legal framework

1.3.1 Para. 10 of the Seventh Schedule to the Banking Ordinance requires AIs to maintain on and after authorization adequate accounting systems and systems of control. These are essential for ensuring prudent and efficient running of the business, safeguarding the assets of the institution, minimising the risk of fraud, monitoring the risks to which the institution is exposed and complying with legislative and regulatory requirements.

1.3.2 Para. 12 of the Seventh Schedule further requires AIs to conduct their business with integrity, prudence, competence and in a manner which is not detrimental to the interests of depositors or potential depositors. As set out in the "Guide to Authorization", the HKMA's assessment of an institution's compliance with this paragraph will take account of, among other considerations, operational risk issues such as ability to deal with external shocks and unexpected contingencies, competence in resistance to internal and external fraud and avoidance of operational errors, and quality of computer systems and staff.

1.3.3 Moreover, §98 of the Banking Ordinance requires all AIs incorporated in Hong Kong to maintain a capital adequacy ratio of not less than 8%. The ratio will take into account an AI's operational risk in addition to credit risk and market risk when Basel II is implemented in Hong Kong.

1.4 Implementation

1.4.1 The HKMA recognises that operational risk management as a separate discipline remains at an early stage of

development compared with some other areas of risk management. The various techniques and tools used to identify, assess, monitor and report operational risk exposures are still evolving. The guidance therefore sets out "sound practices" rather than "statutory requirements" on operational risk management. AIs are expected to develop operational risk management framework consistent with the guidance in this module and commensurate with their size, complexity, and risk profile.

1.4.2 AIs intending to use the STO Approach (or ASA Approach) to calculate the capital charge for their operational risk need to consider the guidance where appropriate in assessing their compliance with the qualitative criteria for using such approaches.

2. Supervisory approach to operational risk

2.1 Objectives and principles

2.1.1 Each AI should develop and maintain an appropriate operational risk management framework that is effective and efficient in identifying, assessing, monitoring and controlling/mitigating operational risk. Each institution will need to consider its complexity, range of products and services, organisational structure, and risk management culture as it develops its operational risk management framework.

2.1.2 The HKMA adopts a risk-based supervisory approach (see SA-1 "Risk-based Supervisory Approach") which enables continuous supervision of AIs' operational risk through a combination of on-site examinations, off-site reviews and prudential meetings. The objective is to assess, among other things, the level and trend of the AI's operational risk exposures and losses as well as the adequacy and effectiveness of its operational risk management framework. In the case of a locally incorporated AI, the HKMA will also assess the adequacy of its capital relative to the size of its exposure.

2.1.3 In assessing an AI's exposure to and management of operational risk, the HKMA will have particular regard to the following factors:

- the appropriateness of the AI's operational risk management framework, including the level of oversight exercised by the Board of Directors and senior management, and risk culture;
- the adequacy of strategies, policies and procedures for managing operational risk, including the definition of operational risk;
- the adequacy of the operational risk management processes in identifying, assessing, monitoring and controlling operational risks;
- the effectiveness of the AI's operational risk mitigation efforts;
- the adequacy and results of the AI's internal review and audit of operational risk;
- the findings and recommendations made in the management letter issued by the AI's external auditors;
- the causes and impacts of significant operational risk events of the AI;
- the AI's procedures for the timely and effective resolution of operational risk events and vulnerabilities; and
- the quality and comprehensiveness of the AI's disaster recovery and business continuity plans.

2.1.4 The HKMA will also seek to ensure that AIs make sufficient public disclosure to allow market participants to assess their approach to operational risk management. In this connection, more guidance will be set out in the supervisory guideline on the disclosure requirements for AIs for implementation of Basel II.

2.2 Supervisory processes

2.2.1 Every AI is subject to the examination of the effectiveness of its operational risk management framework by the HKMA. In addition, the HKMA has the power under §59(2) of the Banking Ordinance to require external auditors' reports to be submitted on an ad hoc basis covering AIs' internal control systems.

2.2.2 In determining the minimum capital adequacy ratio to be observed by a locally incorporated AI under §98 of the Banking Ordinance, the HKMA currently takes into account the AI's exposure to operational risk. Methodology for calculating a specific capital charge for operational risk of locally incorporated AIs will be set out in the Banking (Capital) Rules prescribed by the MA under the Banking Ordinance.

2.2.3 AIs are expected to notify the HKMA of any event(s) that may have a significant impact on their operations. Such events may include:

- a significant operational loss/exposure that has been incurred/identified;
- a significant failure in their systems or controls;
- an intention to enter into an insourcing/outsourcing arrangement in respect of a banking related business area (including back office activities), or to make changes to or amend the scope of their insourcing/outsourcing of such areas;
- any significant changes in organisation, infrastructure or business operating environment; and
- the invocation of a business continuity plan.

2.2.4 Upon receiving notification of the above events, and if the situation as determined by the HKMA warrants, the HKMA may require the reporting AI to submit a report to it analysing the causes/purposes and impacts of the event as well as setting out the action plan to rectify any weaknesses identified or the contingency plan in dealing with failure in an intended change.

2.2.5 Serious lapses or deficiencies in internal controls of an institution can constitute an unsafe and unsound practice and possibly lead to significant losses or otherwise compromise the financial integrity of the institution. If appropriate, the MA will initiate supervisory actions if material deficiencies or situations that threaten the safe and sound conduct of the institution's activities are not adequately addressed in a timely manner. Such supervisory actions may include the requirement of an independent special review report on the problem area,

attachment of a condition to the consent of authorization limiting the level of business activity involved, or suspension of the activity completely, enforcement actions against the institution or its responsible directors and managers, or both, and would require the immediate implementation of all necessary corrective measures.

3. Operational risk management framework

3.1 Overview

3.1.1 In the past, AIs relied primarily on internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. Recently, sound operational risk management is developing into a functional discipline with dedicated staff using established formal policies and processes. This is driven by a growing recognition by the Boards and senior management of the need to address operational risk as a distinct class of risk such as credit risk and market risk for increased risk awareness, protection of reputation, reduced losses, and ultimately protection and enhancement of shareholder value.

3.2 An appropriate framework

3.2.1 Regardless of its size or complexity, each AI is expected to develop an appropriate framework for managing operational risk. The objective of an operational risk management framework is to ensure that operational risks are consistently and comprehensively identified, assessed, mitigated/controlled, monitored and reported.

3.2.2 For the purpose of this guidance, an appropriate operational risk management framework is considered to consist of these components:

- organisational structure (including Board oversight, senior management responsibilities, roles of business line management, an operational risk management function and internal audit);
- risk culture;
- strategy and policy (operational risk management strategy, policies and procedures); and

- operational risk management process (the processes to identify, assess, monitor, control/mitigate and report operational risk).

3.2.3 In practice, an AI's operational risk framework must reflect the scope and complexity of business lines, as well as the corporate organisational structure. Each AI's operational risk profile is unique and requires a tailored risk management approach appropriate for the scale and materiality of the risks present, and size of the institution. There is no single framework that would suit every institution; different approaches will be needed for different institutions. In fact, the banking industry and supervisory authorities continue to develop their organisational models and techniques for operational risk management.

4. Organisational structure

4.1 Overview

4.1.1 Operational risk management requires the attention and involvement of a wide variety of organisational components, each of which has different responsibilities. It is essential that each of the organisational components clearly understands its roles, authority levels and accountabilities under the institution's organisational and risk management structure. All business and support functions should be an integral part of the overall operational risk management framework. The establishment of an independent centralised risk management function can assist the Board and senior management in meeting their responsibility for understanding and managing operational risk. Moreover, although certain staff may be charged with specific responsibilities in relation to operational risk, all staff of the institution should play a role in the identification and management of operational risk.

4.2 Board oversight

4.2.1 Responsibility for operational risk management ultimately rests with the Board of an AI. To discharge this responsibility, the Board, or its delegated committee, should:

- understand the major aspects of the AI's operational risk as a distinct category of risk that should be managed;
- define the operational risk strategy and ensure that the strategy is aligned with the AI's overall business objectives;
- approve and periodically review the AI's corporate framework to explicitly manage operational risk, which aims to establish a common definition of operational risk of the AI, the AI's principles concerning operational risk management and a common risk management framework, and clear governance and reporting structures for operational risk including roles and responsibilities, standards and tools;
- review periodic high-level reports on the institution's overall operational risk profile, which identify material risks and strategic implications for the institution;
- ensure that the senior management is taking necessary steps to implement appropriate policies, processes and procedures within the institution's different lines of business, based on the principles under the Board-approved risk management framework;
- review the risk management framework regularly to ensure that the AI is managing the operational risks from external market changes and other environmental factors, as well as the operational risks associated with new products, activities or systems;
- ensure that the AI's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff; and
- ensure compliance with regulatory disclosure requirements on operational risk.

4.3 Senior management responsibilities

4.3.1 Senior management should have the responsibility for implementing the operational risk management framework approved by the Board. Specifically, they are responsible for developing specific policies, processes and procedures for managing operational risk in all of the AI's material products, activities, processes and systems.

4.3.2 In order to ensure that operational risk policies and procedures are clearly understood and executed, senior management should define the AI's organisational structure for operational risk management and communicate individual roles and responsibilities. It is essential that staff at all levels in the institution clearly understand their individual roles in the operational risk management process.

4.3.3 While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively. They should also ensure that staff responsible for monitoring and enforcing compliance with the AI's operational risk policy have authority independent from the units they oversee. Moreover, senior management should assess the appropriateness of the operational risk management process in the light of the risks inherent in a business unit's activities.

4.3.4 Senior management is also responsible for ensuring that sufficient human and technical resources are devoted for operational risk management such that the AI's activities are conducted by qualified staff with the necessary experience and technical capabilities.

4.4 An operational risk management function

4.4.1 It has become a leading practice of banks to establish a central operational risk management function (at the group and/or corporate level) in a similar manner to institutional credit and market risk functions. The key role of the function is to assist the management in meeting their responsibility for understanding and managing operational risk and to ensure the development and consistent application of operational risk policies,

processes, and procedures throughout the institution. In so doing it performs a number of roles including:

- setting corporate-level policies and procedures concerning operational risk management and controls;
- designing and implementing the institution's operational risk assessment methodology tools and risk reporting system;
- co-ordinating risk management activities across the organisation;
- consolidated reporting to the Board and senior management;
- providing operational risk management training and advising the business units on operational risk management issues, e.g. deployment of operational risk tools; and
- liaising with internal and external audit.

4.4.2 In the case of a branch, subsidiary, or individual business units of a bank with a centralised risk management function at the group and/or corporate level, there will usually be dedicated operational risk staff at the branch, subsidiary or business units to assure consistency of policy and tools, as well as to report results and issues.

4.4.3 The operational risk management function will be more effective if its role is performed by an independent risk function in a similar vein to that for market and credit risk. In practice, the audit function at some institutions may have initial responsibility for developing an operational risk management programme. Where this is the case, AIs should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner. This is to ensure that the independence of internal audit is maintained.

4.4.4 The HKMA recognises that AIs operate in different ways and are using different operational risk management structures and methodologies. Therefore, it does not propose to prescribe a formal definition of an independent operational risk management function. However, in developing their own organisational structures for operational risk management, AIs should consider how

the statures, roles, responsibilities and procedures of different staff functions within the structures can ensure both consistency and completeness in their overall operational risk management.

4.5 Roles of business line management

4.5.1 Business line management is accountable on a day-to-day basis for managing and reporting operational risks specific to their business units. They must ensure that internal controls and practices within their business line are consistent with the AI's firm-wide policies and procedures to support the management of the institution's operational risk. They should ensure that business-specific policies, processes, procedures and staff are in place to manage operational risk for all material products, activities, and processes. Implementation of the operational risk management framework within each business line should reflect the scope of that business line and its inherent operational complexity and operational risk profile. Business line management must be independent of the AI's firm-wide operational risk management function.

4.5.2 To facilitate management of operational risk within each business unit, good practice suggests that there should be dedicated operational risk staff at the business units. These staff members usually have dual reporting lines. While they have a direct reporting relationship in the business unit, they work closely with the central risk management function to assure consistency of policy and tools, as well as to report results and issues. Their responsibilities may include development of risk indicators, determining escalation triggers and providing management reports. To be effective, such staff should be given sufficient empowerment and resources to carry out their responsibilities.

4.6 Other operational risk related functions

4.6.1 There are a number of other operational risk related staff functions within an AI that should play a role in the operational risk management of an AI. These include specialist departments such as legal and compliance, human resources, information technology, and finance, which should be responsible for some specific aspect of operational risk and the related issues, e.g. the human

resources function should be a key participant in the management of "people" risk, rather than merely playing the role of sharing of information and providing of expert advice. These other operational risk related functions should on the one hand be responsible for managing the operational risk in their own area, and on the other provide support to other parties within the organisational structure for operational risk management.

4.7 Role of internal audit

4.7.1 Internal audit should provide an independent assessment of the operational risk management framework, including the functioning of the central operational risk management function. Therefore, it should not have direct operational risk management responsibilities. AIs should have in place adequate audit coverage to verify that operational risk management policies and procedures have been implemented effectively across the AI. The Board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures. Any operational issues identified and reported in the audit process should be addressed by senior management in a timely and effective manner, or raised to the attention of the Board, as appropriate.

5. Risk culture

A successful operational risk management framework, and in particular, effectiveness of the processes in that framework, is depending on a positive risk culture. An AI's risk culture encompasses the general awareness, attitude and behaviour of its employees to risk and the management of risk within the organisation. Factors contributing to a positive risk culture include:

- An AI's business objectives and risk appetite, operational risk management framework and the related roles and responsibilities in implementing the framework must be clearly communicated to staff at all levels, and the staff should understand their responsibilities with respect to operational risk management.
- Senior management must have an ongoing role throughout the risk management process and send out a consistent message to

the whole organisation that they are fully supportive of the risk management framework through their actions and words.

- The Board and senior management should communicate a culture emphasising high standards of ethical behaviour at all levels of the AI. This can be demonstrated through the adoption of a code of conduct[1] and by management setting the example of following it.
- The AI's business and risk management activities must be carried out by qualified staff with the necessary experience, technical capabilities and adequate access to resources.
- The AI's remuneration policies must be consistent with its appetite for risk. Performance incentives should include consideration of risk management and its design should not provide incentives to people to operate contrary to the desired risk management values e.g. established position limits.
- There must be an environment in which staff can speak out and raise operational risk problems openly without fear of negative consequences.

6. Operational risk management strategy, policies and procedures

6.1 Strategy

6.1.1 Operational risk management begins with the determination of the overall strategies and objectives of an institution. Once determined, the institution can identify the associated inherent risks in its strategy and objectives, and thereby establish an operational risk management strategy. Responsibility for defining the operational risk management strategy, and for ensuring it is aligned with overall business objectives, should rest with the Board. In doing so, the Board should provide clear guidance on the AI's risk appetite or tolerance, i.e. what risks the AI is prepared to take in pursuit of its business objectives and what risks are unacceptable.

6.2 Policies

6.2.1 An AI should document its policies for managing operational risk, setting out its strategy and objectives for

[1] For the detailed requirement of a code of conduct please refer to CG-3 "Code of Conduct".

operational risk management for all key underlying businesses and support processes and the processes that it intends to adopt to achieve these objectives. An AI's corporate operational risk policy should be documented and approved by the Board (or its delegated committee) and communicated clearly to staff at all levels.

6.2.2 An AI's corporate policy for managing operational risk should include:

- the definition of operational risk for the institution, including the types of operational risk that are faced by the AI and its customers that the AI will monitor;
- the AI's risk appetite and tolerance for operational risks;
- the approach to identifying, assessing, monitoring, and controlling its operational risks;
- an outline of the reporting framework and types of data/information to be included in the risk management reports; and
- the organisational structure, which defines operational risk management roles, responsibilities and reporting lines of the Board, committees, senior management, risk management function, business line management and other operational risk related functions.

6.2.3 The corporate policy should be supported by a set of principles that apply to specific components of operational risk, such as new customer approval, new product approval, new information technology (IT) systems approval, outsourcing, business continuity planning, crisis management, and money laundering (see para. 7.4.7 for further guidance).

6.2.4 Business line management are responsible for managing risks in their particular business unit. Therefore, they are required to develop supplementary policies and procedures specific to their business, based on and in consistence with the corporate operational risk management policy.

6.3 Definition of operational risk

6.3.1 In order to be able to efficiently identify, assess, monitor and report operational risk within an AI, it is necessary to define the underlying components of operational risk for consistent use across the organisation. The definition should consider the full range of material operational risks facing the institution and capture the most significant causes of severe operational losses. A formal and detailed definition is also essential for improving communications, setting accountability, characterising and accumulating events for modelling and analysis, and consistently sharing experiences and ideas.

6.3.2 The Basel Committee defines operational risk by referring to the four underlying causes of operational risk – process, people, systems and external events (or environment). The definition seeks to delineate operational risks from other risks by referring to key internal and external aspects of a bank's operation that, alone or in combination, can cause operational losses. The following table provides an example of risk cause categories under each of the four underlying causes of operational risk:

Risk Cause Factors	Risk Cause Categories
Process	• Inadequate / inappropriate guidelines, policies & procedures; • Inadequate / failure of communication; • erroneous data entry; • inadequate reconciliation; • poor customer / legal documentation; • inadequate security control; • breach of regulatory & statutory provisions / requirements; • inadequate change management process; and • inadequate back up / contingency plan
People	• breach of internal guidelines, policies & procedures; • breach of delegated

	authority; • criminal acts (internal); • inadequate segregation of duties / dual controls; • inexperienced staff; • staff oversight; and • unclear roles & responsibilities
System	• inadequate hardware / network / server maintenance
External	• criminal acts; • vendor misperformance; • man-made disaster; • natural disaster; and • political / legislative / regulatory causes

6.3.3 Furthermore, to facilitate measuring operational risks and assessing their potential impact, many banks have adopted definitions with categories of risk events (i.e. actual loss or loss events) and effects (i.e. the types of financial implications) to supplement the cause categories. The Basel Committee has developed a matrix with seven broad categories of operational loss event types that are further broken down into sub-categories and related activity examples[2]. Collection and analysis of operational loss data on the basis of these loss event types are required under the AMA Approach of Basel II. In considering and stating their definition of operational risk in their policy, AIs may adopt the Basel matrix as a generic scope. A more detailed definition of operational risk will facilitate assessment, monitoring and reporting of operational risk on a consistent and an aggregate (i.e. group/institution level) basis.

7. Operational risk management process

7.1 Overview

[2] See Annex 7 – Detailed Loss Event Type Classification of Basel II.

7.1.1 AIs should have processes and tools to regularly identify, assess, monitor and control the operational risk inherent in their material products, activities, processes and systems. They should take reasonable steps to ensure that the risk management systems put in place to identify, assess, monitor and control operational risk are adequate for that purpose.

7.2 Risk identification and assessment

7.2.1 In order to better understand its operational risk profile and effectively target risk management resources, an AI should identify the types of operational risk that it is exposed to as far as reasonably possible and assess its vulnerability to these risks. It should identify and assess the operational risk inherent in all existing or new, material products, activities, processes and systems, based on its own definition and categorisation of operational risk. Effective operational risk identification and assessment processes are paramount for the subsequent development of a viable operational risk monitoring and control system.

7.2.2 When identifying its operational risk, an AI should consider both internal and external factors that could adversely affect the achievement of the AI's objectives, such as:

- the AI's management structure, risk culture, human resource management practices, organisational changes and employee turnover;
- the nature of the AI's customers, products and activities, including sources of business, distribution mechanisms, and the complexity and volumes of transactions;
- the design, implementation, and operation of the processes and systems used in the operating cycle of the AI's products and activities; and
- the external operating environment and industry trend, including political, legal, technological and economic factors, the competitive environment and market structure.

7.2.3 Having identified the risks, AIs need to define the appropriate approach to assessing each identified risk,

estimate the probability that the identified risks will materialise by considering the causes of the risks, and assess their impact by referring to the potential effect on the realisation of corporate objectives.

7.2.4 A number of tools are commonly used for identifying and assessing operational risk:

- Self or Risk Assessment – a bank assesses its operations and activities against a menu of potential risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment.
- Risk Mapping – in this process, various business units, organisational functions or process flows are mapped by risk types. This exercise can reveal areas of weakness and help prioritise subsequent management action.
- Risk Indicators – risk indicators are statistics and/or metrics, often financial, which can provide insight into an AI's risk position. These indicators tend to be reviewed on a periodic basis (such as quarterly, monthly) to alert AIs to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

7.2.5 If conducted effectively, self-assessment should result in the identification of control gaps, and consequently the appropriate corrective actions to be taken (or a specific statement to accept the exposure), with a clear indication of the lines of responsibility for implementing the corrective actions and a target completion date. As such, the process should make the risk analysis of an institution explicit, clarify accountability in the line business areas, and ensure oversight by senior management.

7.2.6 In order to understand the effects of its operational risk exposures, an AI should continually assess its operational risks, taking into account factors such as:

- actual operational loss events or events that could have resulted in significant operational losses but

were avoided (e.g. near misses or penalties waived by counterparty as a gesture of goodwill);

- results of internal assessment of risks and controls;
- the figures or trends shown in risk indicators (i.e. quantitative data which can demonstrate operational efficiency, e.g. settlement failures, staff turnover, system downtime, processing volumes and number of errors, or effectiveness of controls, e.g. audit score or number of audit exceptions, limit excesses);
- reported external operational losses and exposures; and
- changes in its business operating environment.

7.2.7 Methodologies to quantify operational risk are developing. As an institution aims to become more sophisticated in quantifying operational risks, complete and accurate data on operational loss events (by categories of risk) and potential sources of operational loss need to be collected. An established and complete loss event database can potentially be used for empirical analysis and modelling of operational risk as well as quantification of the associated loss. Its importance is being recognised for more effective measurement and management of operational risk.

7.3 Risk monitoring and reporting

7.3.1 AIs should implement a process to monitor their operational risk profiles and material exposures to losses on an on-going basis. The process should include both qualitative and quantitative assessment of an AI's exposure to all types of operational risk, assessing the quality and appropriateness of corrective/mitigation actions, and ensuring that adequate controls and systems are in place to identify and address problems before they become major concerns. It should be appropriate to the scale of risks and activities undertaken by the AI.

7.3.2 In monitoring its operational risks, an AI should identify or develop appropriate indicators that provide management with early warning of operational risk issues (often referred to as "key risk indicators" (KRIs)). KRIs used by AIs should provide management with predictive

information and reflect potential sources of operational risk so that management can act on issues before they become major problems to the institution. KRIs are primarily a selection from a pool of operations/control indicators identified and being tracked by various functions of a bank on a periodic basis, which are considered to be relevant for management tracking and escalation triggering. By setting appropriate "goals or limits" or "escalation triggers" to KRIs, monitoring of the KRIs can provide early warning of an increase in operational risk or a breakdown in operational risk management and facilitate communication of potential problems to a higher level of management.

7.3.3 Risk monitoring should be an integrated part of an AI's activities, the frequency of which should reflect the risks involved in an AI's activities as well as the frequency and nature of changes in the operating environment.

7.3.4 The results of an AI's monitoring activities, findings of compliance reviews performed by internal audit and/or the risk management function, management letters issued by external auditors, and reports generated by supervisory authorities, as appropriate, should be included in regular reports to the Board and the senior management to support proactive management.

7.3.5 In general, the Board should receive sufficient high-level information to enable them to understand the AI's overall operational risk profile and focus on the material and strategic implications for the business.

7.3.6 Senior management should ensure that regular management reports on operational risk are received by the relevant level of management, on a timely basis and in a form and format that will aid in the monitoring and control of their business areas. The risk reports to senior management should be from appropriate areas such as business units, support functions, the operational risk management function and internal audit.

7.3.7 Generally, the management reports should contain relevant internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. They should aim to provide information such as:

- the critical operational risks facing, or potentially facing, the institution (e.g. as shown in KRIs and their trend data, changes in risk and control self-assessments, comments in audit/compliance review reports, etc.);
- major risk events/loss experience, issues identified and intended remedial actions;
- the status and/or effectiveness of actions taken; and
- exception reporting (covering among others authorized and unauthorized deviations from the AI's operational risk policy and likely or actual breaches in predefined thresholds for operational exposures and losses).

7.3.8 Reports should be analysed with a view to improving existing management performance as well as developing new risk management policies, procedures and practices.

7.3.9 To ensure the usefulness and reliability of the reports received, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general.

7.3.10 AIs may consider keeping track of the information provided in the reports, particularly the loss data, to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on loss events.

7.4 Risk control and mitigation

7.4.1 AIs should have policies, processes and procedures to control and/or mitigate operational risks. They should also have a system in place for ensuring compliance with a documented set of internal policies concerning the AIs' risk management system. Principle elements of this could include, for example:

- top level reviews of the AI's progress towards the stated objectives;
- checking for compliance with management controls;

- policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
- a system of documented approvals and authorizations to ensure accountability to an appropriate level of management.

7.4.2 AIs should ensure that the risk management control infrastructure keeps pace with growth or changes in the business activity (e.g. new products, operations in branches/subsidiaries remote from head office, and entry into unfamiliar markets).

7.4.3 A critical element to an AI's control of operational risk is the existence of a sound internal control system. When properly designed and consistently enforced, a sound internal control system will help management safeguard the institution's resources, produce reliable financial reports, and comply with laws and regulations. Sound internal controls will also reduce the possibility of significant human errors and irregularities in internal processes and systems, and will assist in their timely detection when they do occur.

7.4.4 Typical practices to control operational risk in an AI include:

- segregation of duties to avoid a conflict of interest in the responsibilities of individual staff which can facilitate concealment of losses, errors or inappropriate actions;
- close monitoring of adherence to assigned risk limits or thresholds and investigation into breaches;
- maintaining safeguards for access to, and use of, bank assets and records;
- ensuring that staff have appropriate expertise and training;
- identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g. where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach); and

- regular verification and reconciliation of transactions and accounts.

7.4.5 For all material operational risks that have been identified, the AI should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled or mitigated, the AI should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

7.4.6 AIs can transfer certain level of their operational risks to third parties through risk mitigation products such as insurance. However, AIs should not view risk mitigation tools as a replacement for internal operational risk controls. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

7.4.7 AIs' operational risk will particularly be driven by the following factors and therefore AIs should have relevant policies and procedures to control their exposures:

- **New products and activities**

  Operational risk can be more pronounced where banks engage in new activities or develop new products, particularly where these activities or products are not consistent with the AIs' core business strategies. Therefore, AIs should have policies in place which set out the standards and describe the roles and responsibilities for the AIs' new product approval process.

  The purpose is to ensure that new business initiatives and changes to the AIs' existing business are introduced in a controlled fashion and that business units and support functions are fully prepared to cope with the proposed new business or changes to existing business. Please see IC-1 "General Risk Management Controls" for some general guidance on the controls over new products/services.

- **IT capability and security and change of IT systems, facilities and equipments**

The policy should aim to ensure that the high risk issues in IT are addressed through adequate IT controls, including security management, system development and change management, information processing, communications network and management of technology service providers. Please refer to TM-G-1 "General Principles for Technology Risk Management" for guidance on general principles which AIs are expected to consider in managing technology-related risks.

- **E-banking services**

  The risk management of e-banking is an integral part of the AI's technology risk management and should cover controls, among others, related to authentication of customers, confidentiality and integrity of information, application security, internet infrastructure and security monitoring, and customer security such as preventive controls relating to fake e-mails or websites. Please refer to TM-E-1 "Supervision of E-banking" for guidance on general principles for risk-management of e-banking.

- **Outsourcing**

  The risk management of outsourcing should cover a comprehensive risk assessment of the proposed outsourcing arrangement in the light of the importance and criticality of the activities to be outsourced, due diligence on the service provider, controls over outsourced activities and contingency planning. Please refer to SA-2 "Outsourcing" on the major points which the HKMA recommends AIs to address when consider outsourcing their activities.

- **Money laundering**

  AIs should have policies, procedures and controls for the fight against money laundering and terrorist financing based on the principles of know your customer, compliance with laws, co-operation with law enforcement agencies, and on-going staff training. To give AIs guidance on the basic policies and principles to combat money laundering and

terrorist financing, the HKMA has issued the Guideline on Prevention of Money Laundering (revised in 2000), Supplement to the Guideline on Prevention of Money Laundering (revised in 2004) and the accompanying Interpretative Notes.

- **Suitability of customers**

  AIs should have policies and procedures for identifying customers whom they consider suitable for selling certain sophisticated, high risk products. The targeted customers should be considered as capable of understanding and bearing the potential financial risks that may rise from such products.

- **Overseas branches/subsidiary offices**

  The operating systems and processes of overseas branches or subsidiaries may change the operational risk profile of AIs. Therefore, AIs should understand the impact of any differences in processes and systems at each of their overseas branches and subsidiaries, and develop appropriate controls over their operations.

- **Customer data privacy**

  As stated in the Code of Banking Practice, AIs should comply with the Personal Data (Privacy) Ordinance in the collection, use and holding of customer information. For details of the principles on customer data privacy, please refer to Guideline 3.7 on "Personal Data (Privacy) Ordinance".

- **External documentation**

  External documentation refers to documents that are produced by AIs and provided to customers and counterparties or third parties, e.g. contracts, transaction statements, or advertising brochures. The presence of inappropriate or inaccurate information in these documents can lead to legal risk and operational risk.

  AIs should have adequate processes and systems to review external documentation prior to issuance. This may include the consideration of:

- compliance with applicable regulatory and legal requirements;
- the extent to which the documentation uses standard terms or non-standard terms;
- the channels or ways in which the documentation is issued; and
- the extent to which confirmation of acceptance is required.

8. Business continuity management and disaster recovery plan

All AIs should have in place formal contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. The management should periodically review these plans so that they are consistent with the AI's current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the AI would be able to execute the plans in the unlikely event of a severe business disruption. Please refer to TM-G-2 "Business Continuity Planning" for the sound practices which the HKMA expects AIs to take in their business continuity planning.

Contents	Glossary	Home	Introduction