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Previous guidelines superseded

OR-1 "Operational Risk Management" (v.1) dated 28.11.05

~~This is a new guideline.~~

Application

To all AIs

Structure

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 inherent~~present~~ in ~~virtually~~ all banking products, ~~bank transactions and~~ activities, processes and systems. It is defined under the capital standards issued by the Basel Committee ~~under its revised framework~~ on Banking Supervision (BCBS)~~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 risks. However, where appropriate, strategic and reputational risks should be considered under an AI's operational risk management framework (ORMF).

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

(a) rely more on increasingly complex automated technology;

(b) develop more complex products;

(c) are involved in large scale mergers and acquisitions;

(d) initiate consolidation and internal reorganisation;

(e) 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

(f) 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 March 2021, the BCBS issued the "Revisions to the

Principles for the Sound Management of Operational Risk" [1] on which this module is primarily based. Superseding the BCBS "Principles for the Sound Management of Operational Risk" issued in 2003 (and revised in 2011 to address lessons from the Global Financial Crisis of 2007 - 09), the 2021 revisions incorporate further guidance to facilitate banks' implementation of the principles, cover other important sources of operational risk, reflect the new operational risk framework in the Basel III reforms, and emphasize the importance of the principles in ensuring operational resilience of banks [2] .~~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:

(a) sets out the HKMA's supervisory approach to operational risk; and

~~(b)~~ provides guidance on the key elements of a sound ORMF~~operational risk management framework; and~~

~~(c)~~(b) ~~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] https://www.bis.org/bcbs/publ/d515.pdf.
[2] Please see the "Principles for operational resilience" issued by the Basel Committee in March 2021 (https://www.bis.org/bcbs/publ/d516.htm).

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

(a) the two sets of 2021 BCBS principles ~~Paper issued by the Basel Committee as~~ mentioned under para. 1.1.4 ~~above~~ and footnote 2;

(b) Principle 25 of the "Core Principles for Effective Banking Supervision"[3]; and

(c) the operational risk management policies and practices adopted by some international banks.

~~• 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.

[3] https://www.bis.org/basel_framework/standard/BCP.htm.

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 its 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 information and communication technology (ICT) [4] ~~computer systems~~ and staff.

1.3.3 Moreover, under ~~§98 of~~ the Banking (Capital) Rules (BCR), any AI ~~Ordinance requires all AIs~~ incorporated in Hong Kong is required to maintain adequate regulatory ~~a~~ capital calculated in accordance with the BCR, taking ~~adequacy ratio of not less than 8%. The ratio will take~~ into account the ~~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 ofdevelopment 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 and implement an ORMF ~~operational risk management framework~~ consistent with the guidance in this module and commensurate with their nature, size, complexity, and risk profile as soon as practicable. The ORMF should be reviewed regularly and kept up to date in the light of the evolving operating environment and operational risk management techniques.

~~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.~~

[4] ICT refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environments.

1.5 Operational resilience

1.5.1 Operational resilience refers to the ability of an AI to deliver critical operations [5] through disruptions. This ability enables an AI to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events, in order to minimize their impact on the delivery of critical operations through disruptions. In considering its operational resilience, an AI should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption [6] under a range of severe but plausible scenarios[7].

1.5.2 Although operational risk management and operational resilience address different goals, they are closely interconnected. An effective operational risk management system and a robust level of operational resilience work together to reduce the frequency and the impact of operational risk events. When implementing the guidance in this module, an AI should also take into account relevant guidance issued by the HKMA in the SPM module OR-2 "Operational Resilience". Specific guidance that links ORMF of an AI to its operational resilience / ability to ensure critical operations delivery through disruptions is set out in paras. 2.2.4, 5.2.1(g), 7.1.1, 7.2.4(f), 7.2.6, 7.4.7(a) & (d), 8.1.3, 8.3.1 (footnote 21) and 8.3.2(a).

2. Supervisory approach to operational risk

2.1 Objectives and principles

2.1.1 Each AI should develop and maintain an appropriate ORMF~~operational risk management framework~~ that is effective and efficient in identifying, assessing, monitoring and controlling/mitigating operational risk, taking into account~~. 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

[5] The term "critical operations" follows the meaning of the same term as defined in OR-2 "Operational Resilience".
[6] The term "tolerance for disruption" follows the meaning of the same term as defined in OR-2 "Operational Resilience".
[7] The term "severe but plausible scenarios" follows the meaning of the same term as defined in OR-2 "Operational Resilience".

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 ORMF, taking into account the guidance set out in this module. ~~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 operational risk 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:

(a) the appropriateness of the AI's ORMF~~operational risk management framework~~, including the level of oversight exercised by the Board of Directors (Board) and senior management, and risk culture;

(b) the adequacy of strategies, policies and procedures for managing operational risk, including the definition of operational risk;

(c) the adequacy of the operational risk management processes in identifying, assessing, monitoring and controlling operational risks;

(d) the effectiveness of the AI's operational risk mitigation efforts;

(e) the adequacy and results of the AI's internal review and audit of operational risk;

(f) the findings and recommendations made in the management letter issued by the AI's external auditors;

(g) the causes and impacts of significant operational risk events of the AI;

(h) the AI's procedures for the timely and effective resolution of operational risk events and vulnerabilities; and

(i) the quality and comprehensiveness of the AI's disaster recovery and business continuity plans.

2.1.4 Where necessary, the HKMA will coordinate and exchange information with other relevant supervisors to facilitate the

evaluation of an AI's ORMF.

~~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 ORMF~~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~~ The HKMA also monitors a locally incorporated AI's compliance with the capital requirements~~AI~~ under ~~§98 of~~ the BCR, taking~~Banking Ordinance, the HKMA currently takes~~ into account the AI's exposure to operational risk. Methodology for calculating the~~a specific~~ capital charge for operational risk is~~of locally incorporated AIs will be~~ set out in the BCR~~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) a significant operational loss/exposure that has been incurred/identified;

(b) a significant failure in their systems or controls;

(c) 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;

(d) any significant changes in organisation, infrastructure or business operating environment; and

(e) 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~~arising from an intended change. In any case, after an operational risk incident, an AI should assess threats and vulnerabilities that affect the delivery of its critical operations again, taking into account lessons learned and new threats and vulnerabilities that caused the incident. The HKMA also expects that any controls and procedures implemented to address those threats and vulnerabilities should be reviewed from time to time to ensure their continued effectiveness.

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.

2.2.6 An AI should strive to improve its operational risk management framework on an ongoing basis. Where necessary, the HKMA will monitor, compare and evaluate the improvements achieved by an AI and its plans for prospective developments during the course of its risk-based supervision.

3. Operational risk management framework

3.1 Overview

3.1.1 An AI should develop, implement and maintain an ORMF that is fully integrated into its overall risk management processes. The ORMF should be embedded across all levels of the organization including group and business

units [8] as well as new business initiatives, products, activities, processes and systems. In addition, results of the AI's operational risk assessment should be incorporated into its overall business strategy development process.

~~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 ORMF~~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 module~~guidance~~, an appropriate ORMF should contain the major~~operational risk management framework is considered to consist of these~~ components set out below:

(a) risk governance~~organisational structure~~ (including Board and~~oversight,~~ senior management oversight) and risk culture – see section 4;

~~(a)~~(b) risk management structure made up of three lines~~responsibilities, roles~~ of defence, i.e. business line management (first line of defence), independent corporate ~~an~~ operational risk management function (CORF, second line of defence[9]) and independent assurance (third line of defence) – see section 5;~~and internal audit);~~

[8] The term "business unit" is meant broadly to include all associated support, corporate and/or shared service functions, e.g. Finance, Human Resources and Operations and Technology. However, Risk Management and Internal Audit are not included unless otherwise specifically indicated.

[9] In addition to a CORF, the second line of defence also typically includes a Compliance function.

- ~~risk culture;~~

~~(b)~~(c) ~~strategy and policy (~~operational risk management strategy, policies and procedures – see section 6;~~);~~ ~~and~~

~~(c)~~(d) operational risk management process ~~(the processes~~ to identify, assess, monitor, control/mitigate and report operational risk – see section 7;~~).~~

(e) specific aspects of operational risk management including change management, ICT and business continuity planning – see section 8; and

(f) disclosure – see section 9.

3.2.3 In practice, an AI's ORMF~~operational risk framework~~ must reflect the scope and complexity of business lines, range of products and services,~~as well as the~~ corporate organisational structure, and risk management culture. 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.~~

3.2.4 Nevertheless, the three lines of defence model has been widely adopted in the industry with varied degrees of implementation formality. AIs should adopt this model adequately and proportionately to manage every kind of operational risk subcategory, including ICT risk, and be able to demonstrate that the model is operating satisfactorily and to explain how the Board (or an independent committee of the Board) and senior management ensure that the model is implemented and operating in an appropriate manner. They should ensure that each line of defence:

(a) is adequately resourced in terms of budget, tools and staff;

(b) has clearly defined roles and responsibilities;

(c) is continuously and adequately trained;

(d) promotes a sound risk management culture across the AI; and

(e) communicates with the other lines of defence to reinforce the ORMF.

3.2.5 The components of the ORMF should be fully integrated into the overall risk management processes of the AI by the first line of defence, adequately reviewed and challenged by the second line of defence, and independently reviewed by the third line of defence.

3.2.6 If in one business unit there are functions of both the first and second line of defence, the AI should document and distinguish the responsibilities of such functions in the first and second line of defence, emphasising the independence of the second line of defence.

4. Risk governance
~~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 ORMF. ~~operational risk management framework.~~ The establishment of a CORF~~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 The ~~R~~responsibility for operational risk management ultimately rests with the Board of an AI. To discharge this responsibility, the Board~~,~~ (or its delegated committee)~~,~~ should approve and periodically review the following:

(a) the ORMF; and

(b) the risk appetite and tolerance statement and risk limits for operational risk.

ORMF

4.2.2 To ensure that the ORMF is suitable and will be working effectively for the AI, the Board or its delegated committee(s) should:

(a) understand the nature and complexity of the risks inherent in the portfolio of the AI's products, services, activities, and systems;

(b) establish a risk culture and ensure that the AI has adequate processes for understanding the nature and scope of the operational risk inherent in its current and planned strategies and activities;

(c) establish clear lines of management responsibility and accountability for implementing a strong internal control environment with appropriate independence/segregation of duties between CORF, business units and support functions;

(d) ensure that the operational risk management processes are subject to comprehensive and dynamic oversight and are fully integrated into, or coordinated with, the overall framework for managing all risks across the AI;

(e) provide senior management with clear guidance regarding the principles underlying the ORMF, and approve the corresponding policies developed by senior management under these principles;

(f) regularly review and evaluate the ORMF's effectiveness to ensure that the AI has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems (including in relation to the application of ICT – see section 8.2), including changes in risk profiles and priorities (e.g. changing business volumes);

(g) ensure that the AI's ORMF is subject to effective independent review by the third line of defence (audit or other appropriately trained independent third parties from external sources); and

(h) ensure that, as best practice evolves, management is availing themselves of these advances.

- ~~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.~~

Risk appetite and tolerance statement and risk limits

4.2.3 The risk appetite and tolerance statement for operational risk should articulate the nature, types and levels of operational risk that the bank is willing to assume. It should be developed under the authority of the Board and linked

to the AI's short- and long-term strategic and financial plans. Taking into account the interests of the AI's customers and shareholders as well as regulatory requirements, an effective risk appetite and tolerance statement should:

(a) be easy to communicate and therefore easy for all stakeholders to understand;

(b) include key background information and assumptions that informed the AI's business plans at the time it was approved;

(c) include statements that clearly articulate the motivations for taking on or avoiding certain types of risk, and establish boundaries or indicators (which may be quantitative or not) to enable monitoring of these risks;

(d) ensure that the strategy and risk limits of business units and legal entities, as relevant, align with the bank-wide risk appetite statement; and

(e) be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the AI understands what events might push it outside its risk appetite and tolerance statement.

4.2.4 The Board should review regularly the risk appetite and tolerance statement and the appropriateness of the operational risk limits. This review should consider the current and expected changes in the external environment (including the regulatory context across all jurisdictions where the institution provides services); ongoing or forthcoming material increases in business or activity volumes; the quality of the control environment; the effectiveness of risk management or mitigation strategies; loss experience; and the frequency, volume or nature of limit breaches. The Board should also monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

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.~~Senior management should develop for approval by the Board a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility for operational risk management.

4.3.2 An AI's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, an AI should take into account the following sound industry practices:

- **Committee structure** – A large and more complex AI establishes one or more operational risk management committees which report to the Board level risk management committee. Depending on the nature, size and complexity of the AI, there may be operational risk committees by country, business or functional area. Smaller and less complex AIs may establish just one risk management committee overseeing all risks without a separate operational risk management committee;
- **Committee composition** – An operational risk management committee (or the risk management committee for a smaller AI) includes members with a variety of expertise, covering business activities, financial activities, legal, technological and regulatory matters and independent risk management;
- **Committee operation** – Committee meeting should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

4.3.3 Senior management is responsible for implementing the ORMF approved by the Board through the development of specific policies, processes and procedures that can be implemented and verified within business units for managing operational risk. Such policies, processes and procedures should be consistently implemented and maintained throughout the organization for the management of operational risk in all of the AI's material products, activities, processes and systems, in alignment with the AI's risk appetite and tolerance statement.

4.3.4 In order to ensure that operational risk management 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.

4.3.5 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 in line with the AI's risk appetite and risk tolerance statement. 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 and ensure the appropriateness of the operational risk management process in the light of the risks inherent in a business unit's activities.

4.3.6 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 and access to resources.

4.3.7 Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing other risks such as credit, market, etc., as well as with those responsible for the procurement of external services such as insurance risk transfer and other third-party arrangements (including outsourcing). Failure to do so could result in significant gaps or overlaps in the AI's overall risk management programme.

4.3.8 Senior management is responsible for establishing and maintaining robust challenge mechanisms and processes for resolving operational issues, including systems to report, track and escalate issues to ensure their resolution.

4.3.9 Since operational risk management is evolving and the business environment is constantly changing, senior

management should ensure that the ORMF (in particular policies, processes and systems) remain sufficiently robust to manage and ensure that operational losses are adequately addressed in a timely manner. Improvements in operational risk depend heavily on senior management's willingness to be proactive and also act promptly and appropriately to address operational risk managers' concerns.

4.3.10 See also CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions" for general guidance on corporate governance.

4.4 Risk culture

4.4.1 The Board and senior management of an AI also have an important responsibility in fostering a positive risk culture on which a successful ORMF (particularly in respect of the effectiveness of the processes in that framework) depends. In general, the Board should take the lead in establishing a strong risk management culture for the AI, which should be implemented by the senior management.

4.4.2 ~~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:

(a) An AI's business objectives and risk appetite, operational risk management framework and the related roles, ~~and~~ responsibilities and authorities of relevant staff in implementing the framework must be clearly set out and communicated by the senior management to ~~staff at~~ all ~~levels, and the~~ staff within the organization in order for them to~~should~~ understand their responsibilities with respect to operational risk management.

(b) The Board and senior management should provide strong and consistent support for operational risk management and ethical behavior, convincingly reinforcing codes of conduct and ethics, compensation strategies and training programmes. Senior management must have an ongoing role throughout the risk management process and send out a consistent message to the whole organisation

that the Board and senior management~~they~~ are fully supportive of the risk management framework through their actions and words.

(c) The Board and senior management should communicate a culture emphasising high standards of ethical behaviour and prohibiting conflicts of interest or inappropriate provision of financial services (whether willful or negligent) at all levels of the AI. This can be achieved~~demonstrated~~ through the establishment and application to both staff and Board members~~adoption of~~ a code of conduct[10], or an ethic policy, and by members of the Board and senior management setting the example of following it. The code or relevant policy should be regularly reviewed and approved by the Board and attested by employees. Its implementation should be overseen by a board level committee and should be made publicly available (e.g. on the AI's website). A separate code of conduct may be established for specific positions in the AI (e.g. treasury dealers and senior management).

~~(d) 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.~~

(d) Senior management should ensure that appropriate operational risk management and ethical behavior training is available at all levels throughout the organization, such as heads of business units, heads of internal controls and senior managers. Training provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

(e) The AI's remuneration policies must be consistent with its appetite and tolerance for risk as well as overall safety and soundness. It must also appropriately balance~~for~~ risk and reward [11]. Performance incentives should include

~~[10] For the detailed requirement of a code of conduct please refer to CG-3 "Code of Conduct".~~

[11] See also BCBS *Report on the range of methodologies for the risk and performance alignment of remuneration*, May 2011; Financial Stability Forum *Principles for sound compensation practices*, April 2009; Financial Stability Board *FSB principles for sound compensation practices – implementation standards*, September 2009 and the Financial Stability Board's toolkit *Strengthening Governance Frameworks to Mitigate Misconduct Risk*, April 2018.

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.

(f) There must be an environment in which staff can speak out and raise operational risk problems openly without fear of negative consequences.

4.4.3 An AI should also refer to the following SPM modules for general guidance relating to sound risk management culture:

(a) CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions";

(b) IC-1 "Risk Management Framework";

(c) CG-3 "Code of Conduct"; and

(d) CG-5 "Guideline on a Sound Remuneration System".

5. Three lines of defence

5.1 Business unit ~~Roles of business line~~ management (first line of defence)

5.1.1 Business unit ~~line~~ management is accountable on a day-to-day basis for identifying, managing and reporting operational risks specific to a business unit. ~~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 ORMF~~operational risk management framework~~ within each business unit~~line~~ should reflect the scope of that business unit~~line~~ and its inherent operational complexity and operational risk profile [12]. Business unit~~line~~ management must be independent of the AI's firm-wide CORF~~operational risk management function~~.

[12] Operational risk profile describes the operational risk exposures and control environment assessments of business units and considers the range of potential impacts that could arise from estimates of expected to severe losses. The profile generally provides management and the Board with a representation of operational risk exposures at a level which supports their decision-making and oversight responsibilities.

5.1.2 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 CORF~~central risk management function~~ to assure consistency of policy and tools, as well as to report results and issues. The~~Their~~ responsibilities of the first line of defence ~~may include development of risk indicators, determining escalation triggers and providing management reports. To be effective, such staff~~ should include:~~be given sufficient empowerment and resources to carry out their responsibilities.~~

(a) identifying and assessing the materiality of operational risks inherent in their respective business units through the use of operational risk management tools;

(b) establishing appropriate controls to mitigate inherent operational risks, including business-specific policies, processes, procedures and systems, and assessing the design and effectiveness of these controls through the use of the operational risk management tools;

(c) reporting whether the business units lack adequate resources, tools and training to ensure identification and assessment of operational risks;

(d) monitoring and reporting the business units' operational risk profiles, and ensuring their adherence to the established operational risk appetite and tolerance statement; and

(e) reporting residual operational risks not mitigated by controls, including operational loss events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances.

5.2 Operational~~An operational~~ risk management function (second line of defence)

5.2.1 It has become a leading practice of banks to establish a CORF~~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 senior~~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 (see section 7) throughout the institution. In so doing CORF~~it~~ performs a number of roles including:

(a) developing and maintaining~~setting~~ corporate-level policies, ~~and~~ procedures and guidelines for~~concerning~~ operational risk management and controls;

(b) designing and implementing the institution's operational risk assessment methodology tools and risk reporting system;

(c) developing an independent view regarding business unit's (i) identified material operational risks, (ii) design and effectiveness of key controls, and (iii) risk tolerance;

~~-~~challenging the relevance and consistency of the business unit's implementation of the operational~~co-ordinating~~ risk management tools, measurement activities and~~across the organisation;~~

(d) ~~consolidated~~ reporting systems, and providing evidence that such challenge is conducive to the evaluation of its effectiveness;

(e) establishing unified classification, methodology and procedures of operational risk;

~~(d)~~(f) reviewing and contributing to the monitoring and reporting of the operational risk profile to the Board and senior management;

(g) working alongside other relevant functions to manage and address any risks that threaten the delivery of critical operations and coordinating business continuity planning, third-party dependency management, recovery and resolution planning and other relevant risk management frameworks to strengthen operational resilience across the institution;

~~(e)~~(h) designing and providing operational risk management training, including to instill risk awareness, and advising the business units on operational risk management issues, e.g. deployment of operational risk tools; and

~~(f)~~(i) liaising with internal and external audits.

5.2.2 The managers of the CORF should be of sufficient stature within the AI to perform their duties effectively. Ideally, they are assigned a title that is commensurate with other risk management functions such as those on credit, market and liquidity risks.

5.2.3 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 for~~of~~ a~~n independent~~ CORF~~operational risk management function~~. However, ~~in developing their own organisational structures for operational risk management,~~ AIs should in any case have a policy which clearly defines the~~consider how the statures,~~ roles and~~,~~ responsibilities of the CORF, reflective~~and procedures~~ of ~~different staff functions within~~ the size~~structures can ensure both consistency~~ and complexity of their operations.~~completeness in their overall operational risk management.~~

5.2.4 In general, the CORF in larger AIs is expected to have a reporting structure independent of the risk-generating business units and be responsible for the design, maintenance and ongoing development of the ORMF within the AI. For smaller AIs, independence of the ORMF may be achieved through separation of duties and independent review of processes and functions.

5.2.5 In practice, the internal audit function in some AIs~~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 to it 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.

5.2.6 In the case of a branch, subsidiary, or individual business units of an AI~~a bank~~ with a CORF~~centralised risk management function~~ at the group and/or corporate level, there should~~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.

5.2.7 As appropriate, the ORMF documentation should clearly reference the relevant operational risk management policies and procedures.

5.3 Other operational risk related functions

5.3.1 The CORF typically engages relevant corporate control groups to support its assessment of the operational risks and controls. There are a number of other operational risk related staff functions within an AI that should play a supporting role to CORF in the operational risk management of an AI. These include specialist departments of ~~such as~~ legal and compliance, human resources, ICT~~information technology~~, and finance, etc., which should be responsible for some specific aspects 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 hand provide support to other parties within the organisational structure for operational risk management.

5.4 Independent assurance (third line of defence)~~Role of internal audit~~

5.4.1 ~~Internal audit~~The Board should be provided~~provide an~~ independent assurance regarding the appropriateness of an AI's ORMF. The relevant assessment should be performed by parties such as the internal auditors, external auditors or other suitably qualified independent third parties, who are not involved in the development, implementation and day-to-day ~~of the~~ operational risk management processes~~framework, including~~ or the operations~~functioning~~ of the other two lines of defence. ~~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.~~

5.4.2 An effective independent assessment should:

(a) review the design and implementation of the operational risk management systems and associated governance processes through the first and second lines of defence (including the independence of the second line of defence);

(b) review validation[13] processes to ensure they are independent and implemented in a manner consistent with established policies;

(c) ensure that business unit management promptly, accurately and adequately respond to the issues raised, and regularly report to the Board or its relevant committees on pending and closed issues; and

(d) opine on the overall appropriateness and adequacy of the ORMF and the associated governance processes across the AI, including whether the ORMF meets organisational needs and expectations (such as in respect of the corporate risk appetite and tolerance, and adjustment of the framework to changing operating circumstances) and complies with statutory and legislative provisions, contractual arrangements, internal rules and ethical conduct.

5.4.3 Any operational issues identified and reported in the assessment process should be addressed by senior management in a timely and effective manner, or raised to the attention of the Board, as appropriate.

5.4.4 As appropriate, the CORF should assess and propose control measures to manage the operational risk inherent in the third line of defence.

[13] Validation is critical for a well-functioning ORMF in that it ensures that the quantification systems used by an AI are sufficiently robust and provide assurance of the integrity of inputs, assumptions, methodologies, processes and outputs, resulting in assessments of operational risk that credibly reflect the operational risk profile of the AI.

~~5. Risk culture~~

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 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:

(a) the definition of operational risk (see section 6.3) and operational loss 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~~

(b) the ~~organisational~~ governance structure, which defines operational risk management roles,

responsibilities and reporting lines of the Board, committees [14], senior management, risk management function, business line management and other operational risk related functions;~~.~~

(c) the AI's accepted operational risk appetite and tolerance; the thresholds, material activity triggers or limits for inherent operational risk (i.e. the risk before controls are considered) and residual operational risk (i.e. the risk exposure after controls are considered); and the approved risk mitigation strategies and instruments;

(d) the tools for risk and control identification and assessment and the role and responsibilities of the three lines of defence in using them;

(e) the approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure and ensuring controls are designed, implemented and operating effectively;

(f) the inventory risks and controls implemented by all business units (e.g. in a control library);

(g) a common taxonomy of operational risk terms (see further elaboration in para. 6.3.1);

(h) an outline of the management reporting framework for producing timely and accurate data/information and the types of data/information to be included in the risk management reports;

(i) a mechanism for independent review and challenge of the outcome of the operational risk management process; and

(j) a requirement that the policy will be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the operational risk profile of the AI occurs.

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, ICT~~new information technology (IT)~~ systems

[14] Mandates and memberships of the relevant committees should also be available.

approval, outsourcing, business continuity planning, crisis management, and money laundering (see para. 7.4.7 for further guidance).

6.2.4 Business unit~~line~~ management is~~are~~ responsible for managing risks in a~~their~~ particular business unit. Therefore, it is~~they are~~ required to develop supplementary policies and procedures specific to its~~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~~. In this connection, a common taxonomy of operational risk terms should be provided in the policy to ensure consistency of risk identification, exposure rating and risk management objectives across all business units[15]. The taxonomy should distinguish operational risk exposures by event types, causes, materiality and business units where they occur. It should also flag those operational exposures that partially or entirely represent legal, conduct, model, ICT (including cyber) risks as well as exposures in the credit or market risk boundary.

~~6.3.1~~6.3.2 The definition of operational risk 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~~6.3.3 The BCBS~~Basel Committee~~ defines operational risk by referring to the four underlying causes of operational risk – process, people, systems and external events (or environment) (see para. 1.1.2). The definition seeks to delineate operational risk~~s~~ from other risks by referring to key internal and external aspects of a bank's operations that, alone or in combination, can cause operational losses. The following table provides an example of risk cause

[15] An inconsistent taxonomy of operational risk terms may increase the likelihood of failure to identify and categorise risks, or failure to allocate responsibility for the assessment, monitoring, control and mitigation of risks.

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~~6.3.4 Furthermore, to facilitate managing and measuring operational risks and assessing the~~their~~ potential impact~~, many banks have adopted definitions with categories~~ of

operational~~risk events (i.e. actual~~ loss events, an AI should classify those ~~or loss~~ events into predetermined event ~~)~~ ~~and effects (i.e. the~~ types~~. of financial implications) to supplement the cause categories.~~ The BCBS~~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[16] ~~[17]~~ as set out in Annex. If an AI's internal classification system is different from that of the BCBS, it should document its criteria for mapping its internal classification with the broad event type categories (level 1) set out in the Annex. An AI should provide its loss data with mapping to the broad event types in the Annex to the HKMA for inspection upon request.~~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

7.1.1 AIs should have effective means ~~processes and tools~~ to regularly identify, assess, monitor and control the operational risk inherent in their material products, activities, processes and systems in a timely manner, which should ensure that potential risks, threats and vulnerabilities that may affect critical operations delivery are prevented. ~~They should take~~ Reasonable steps should be taken to ensure that these processes and tools ~~the risk management systems put in place to identify, assess, monitor and control operational risk~~ are adequate and effective for the ~~that~~ purposes.

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 risks to which~~risk that~~ it is

[16] See Basel consolidated framework OPE25.17 Table 2.
[17] ~~See Annex 7 – Detailed Loss Event Type Classification of Basel II.~~

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 are fundamental characteristics~~processes are paramount for the subsequent development~~ of an effective~~a viable~~ operational risk management~~monitoring and control~~ system, and directly contribute to operational resilience capabilities.

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:

(a) the AI's management structure, risk culture, human resource management practices, organisational changes and employee turnover;

(b) the nature of the AI's customers, products and activities, including sources of business, distribution mechanisms, and the complexity and volumes of transactions;

(c) the design, implementation, and operation of the processes and systems used in the operating cycle of the AI's products and activities; and

(d) 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:

(a) **Event management** (the process of identification, analysis, end-to-end management and reporting of an operational risk event that follows a pre-determined set of protocols) – A sound event management approach typically includes analysis of events to identify new operational risks,

understanding the underlying causes and control weaknesses, and formulating an appropriate response to prevent recurrence of similar events. This information is an input to self-assessments (see (c) below) and, in particular, to the assessment of control effectiveness.

(b) **Operational risk event data** (a comprehensive operational risk event dataset that collects all material events experienced by an AI and serves as a basis for operational risk assessments) – The event dataset typically includes internal loss data and near misses. Event data is typically classified according to a taxonomy defined in the ORMF policies and consistently applied across the AI. Event data typically include the date of the event (occurrence date, discovery date and accounting date) and, in the case of loss events, financial impact. Where available, other root cause information for the events should ideally also be included in the operational risk dataset. Where feasible, AIs should also seek to gather external operational risk event data and use the data in their internal analysis, as it is often informative of risks that are common across the industry.

(c) **Self-assessments** (assessments of operational risks and controls on various different levels conducted by the AI) – The assessments typically evaluate inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered) and contain both quantitative and qualitative elements. The qualitative element reflects consideration of both the likelihood and consequence of the risk event in the bank's determination of its inherent and residual risk ratings. The assessments may utilise business process mapping to identify key steps in business processes, activities, and organisational functions, as well as the associated risks and areas of control weakness. The assessments should contain sufficiently detailed information on the business environment, operational risks, underlying causes, controls and evaluation of control effectiveness to enable an independent reviewer to determine how the bank reached its ratings. A risk register can be

maintained to collate this information to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, risk committees and the Board.

(d) **Control monitoring and assurance framework** (a structured approach to the evaluation, review and ongoing monitoring and testing of key controls) – The analysis of controls ensures they are suitably designed for the identified risks and operating effectively. The analysis should also consider the sufficiency of control coverage, including adequate prevention, detection and response strategies, taking into account different operational risks across business areas.

(e) **Metrics** (quantitative indicators developed using operational risk event data and risk and control evaluations to assess and monitor operational risk exposure) – Metrics are primarily selected operation/control indicators considered relevant for management tracking and escalation triggering. They may be simple indicators that are identified and periodically tracked by various functions of an institution, such as event counts, or outputs from more sophisticated exposure models as appropriate. The intention of metrics is to provide early warning information to monitor ongoing performance of the business and the control environment, and to report the operational risk profile, so that management can act on issues before they become major problems to an institution. Effective metrics clearly link to the associated operational risks and controls. Monitoring metrics and related trends through time against agreed thresholds or limits provides valuable information for risk management and reporting purposes.

(f) **Scenario analysis** (a method to identify, analyse and measure a range of scenarios, including low probability and high severity events (e.g. pandemics, natural disasters, and failures or disruptions at a third party or within the third party's supply chain, etc.), some of which could result in severe operational risk losses) – Scenario analysis typically involves workshop meetings of subject matter experts including senior management,

business management and senior staff responsible for operational risk management and other functional areas such as compliance, human resources and IT risk management, to develop and analyse the drivers and range of consequences of potential events. Inputs to the scenario analysis would typically include relevant internal and external loss data, information from self-assessments, the control monitoring and assurance framework, forward-looking metrics, root-cause analyses and the process framework, where used. The scenario analysis process could be used to develop a range of consequences of potential events, including impact assessments for risk management purposes, supplementing other tools based on historical data or current risk assessments. It could also be integrated with disaster recovery and business continuity plans, for use within testing of operational resilience (also see OR-2 "Operational Resilience"). Given the subjectivity of the scenario process, a robust governance framework and independent review are important to ensure the integrity and consistency of the process.

(g) **Benchmarking and comparative analyses** (comparisons of the outcomes of different risk measurement and management tools deployed within the AI, as well as comparisons of metrics from the AI to other firms in the industry) – Such comparisons can be performed to enhance understanding of the AI's operational risk profile. For example, comparing the frequency and severity of internal losses with self-assessments can help the AI determine whether its self-assessment processes are functioning effectively. Scenario data can be compared to internal and external loss data to gain a better understanding of the severity of the AI's exposure to potential risk events.

- ~~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 AIs should ensure that the operational risk assessment tools' outputs are:

(a) based on accurate data, whose integrity is ensured by strong governance and robust verification and validation procedures;

(b) adequately taken into account in the internal pricing and performance measurement mechanisms as well as for business opportunities assessments; and

(c) subject to CORF-monitored action plans or remediation plans when necessary.

7.2.6 The operational risk assessment tools cited in para. 7.2.4 can also directly contribute to an AI's operational resilience approach. In particular, event management, self-assessment and scenario analysis procedures allow AIs to identify and monitor threats and vulnerabilities to their critical operations. AIs should use the outputs of these tools to improve their operational resilience controls and procedures[18].

~~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~~

[18] These controls and procedures should be consistent with and conducted alongside the identification of threats and vulnerabilities as part of an AI's operational resilience approach.

~~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 make use of appropriate metrics (referred to in paragraph 7.2.4(e)). ~~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~~the metrics, monitoring of the ~~KRIs~~metrics 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 pace~~frequency~~ and nature of changes in the operating environment.

7.3.4 The results of an AI's monitoring activities, assessments~~findings~~ of the ORMF~~compliance reviews~~ performed by internal/external 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 An AI should be able to produce timely reports in both normal and stressed market conditions[19]. The reports should be comprehensive, accurate, consistent and actionable across business units and products. To this end, the first line of defence should ensure reporting on any residual operational risks, covering operational risk events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances. Reports should be manageable in scope and volume by providing an outlook on the AI's operational risk profile and adherence to the operational risk appetite and tolerance

[19] Reporting should be consistent with the BCBS's Principles for effective risk data aggregation and risk reporting (https://www.bis.org/publ/bcbs239.pdf).

statement. Effective decision-making is impeded by both excessive amounts and paucity of data.

~~7.3.5~~7.3.6 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.

7.3.7 Generally, the management reports should describe the operational risk profile of an AI by providing ~~contain relevant~~ internal financial, operational, and compliance indicators~~data~~, as well as external market or environmental information about events and conditions that are relevant to decision making. They should aim to provide information such as:

(a) the ~~critical~~key and emerging operational risks facing, or potentially facing, the institution (e.g. as shown in ~~KRIs~~metrics and their trend data, changes in risk and control self-assessments, comments in audit/compliance review reports, etc.);

~~•~~ major internal operational risk events~~/loss experience, issues identified~~ and losses (including root causes, ~~intended remedial actions;~~

(b) the status and/or effectiveness of remedial actions taken); ~~and~~

(c) relevant external events or regulatory changes, and any potential impact on the AI; and

~~(c)~~(d) exception reporting (covering, among others, authorized and unauthorized deviations from the AI's operational risk policy (including in terms of risk appetite and risk tolerance) and likely or actual breaches in predefined thresholds, limits or qualitative requirements for operational exposures and losses).

~~7.3.6~~7.3.8 Data capture and risk reporting processes~~Reports~~ should be analysed periodically with the goal of enhancing risk~~a view to improving existing~~ management performance as well as advancing~~developing new~~ risk management policies, procedures and practices.

~~7.3.7~~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.

~~7.3.8~~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 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 ensure the efficiency and effectiveness of the operations, 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.

7.4.2 For all material operational risks that have been identified, the AI should decide whether to use appropriate policies, processes, procedures and systems 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.

7.4.3 A sound internal control programme consists of risk assessment, activities monitoring and control, communication and information[20], which are also integral components of the risk management process. Typical practices to control operational risk in an AI include:

(a) clearly established authorities and/or processes for approval;

(b) 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) should be identified, avoided or minimized to the extent possible. Conflict of interest that cannot be avoided in practice should be subject to dual controls (e.g. a process that uses two or more separate entities/persons operating in concert to protect sensitive functions or information) or other countermeasures, independent monitoring

[20] Management should make clear the internal control requirements to individual functions, which in turn provide information and feedback to enhance the control requirements on an ongoing basis.

and review to guard against concealment of losses, errors or other inappropriate actions;

(c) close monitoring of adherence to assigned risk limits or thresholds and investigation into breaches;

(d) ~~maintaining~~ safeguards for access to, and use of, bank assets and records;

(e) appropriateness of ~~ensuring that~~ staff level ~~have appropriate expertise~~ and training to maintain technical expertise;

(f) ongoing processes to identify~~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~~

(g) regular verification and reconciliation of transactions and accounts~~.~~; and

(h) vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks, or another period commensurate with the role of the employee and the risk profile / complexity of the AI.

7.4.4 The control processes and procedures should include a system for ensuring compliance with the policies regulations and laws. ~~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:

(a) top level reviews of the AI's progress towards the stated objectives;

(b) verification of~~checking for~~ compliance with management controls;

(c) ~~policies, processes and procedures concerning the~~ review of the~~,~~ treatment and resolution of instances of non-compliance ~~issues~~; ~~and~~

(d) evaluation of the required~~a system of documented~~ approvals and authorizations to ensure accountability to an appropriate level of

management; and.

(e) tracking of reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy, regulations and laws.

7.4.27.4.5 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).

7.4.6 Control process and procedures should be consistent with the AI's operational resilience approach so that through the due diligence exercised by respective functions (i.e. the three lines of defence), the operational resilience of the AI can be maintained in both normal circumstances and in the event of disruptions.

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:

(a) **~~New products and activities~~Change initiatives**

Operational risk can be more pronounced where ~~banks~~ AIs initiate changes, such as engaging~~e~~ in new activities or developing new products/services, entering into unfamiliar markets/jurisdictions, implementing new or modified business processes or technology systems, and/or engaging in businesses that are geographically distant from the head office. ~~particularly where these activities or products are not consistent with the AI's core business strategies.~~ Therefore, AIs should have policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change, and ~~in place which set out the standards and~~ describing~~e~~ the roles and responsibilities for parties involved in the change management~~the AIs' new product approval~~ process. The policies should set out objective criteria with respect to the approval of change initiatives.

The purpose is to ensure that ~~new business~~ change 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~~. In addition, AIs should leverage on their change management capability as a way to assess potential effects of planned changes to any underlying components for the delivery of critical operations and on their interconnections and interdependence.

See section 8.1 for further guidance on the change management process and section 4.3 of ~~Please see~~ IC-1 "~~General~~ Risk Management ~~Controls~~Framework" for ~~some~~ general guidance on the controls over new products/services.

(b) **Use of ICT~~IT capability and security and change of IT systems, facilities and equipments~~**

The policy should aim to ensure that the ~~high~~ risk~~s issues in IT~~associated with the use of ICT are addressed through adequate ICT governance and ~~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 and section 8.2 below for further guidance on ~~which AIs are expected to consider in managing technology-related risks~~ICT risk management.

(c) **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~~fraudulent bank websites, phishing e-mails or ~~websites~~similar scams. Please refer to TM-E-1 "~~Supervision~~ Risk Management of E-banking" for general guidance on ~~general~~ principles for risk ~~-~~management of e- banking.

(d) **~~Outsourcing~~Third-party dependencies**

While resorting to entities such as third party service providers can help manage costs, provide expertise, expand product offerings and improve

services, it also introduces risks. The Board and senior management should understand such risks and ensure that proper policies and procedures are in place to address the risks associated with third party service providers whether there exists an outsourcing arrangement or the AI is otherwise relying on the service providers to carry out its operations. For outsourced activities, t~~T~~he risk management process ~~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, concentration of risk, complexity of the outsourcing, 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 considering to outsource~~ing~~ their activities. Moreover, an AI should take into account the access right of the resolution authorities in its outsourcing arrangements. The risk management policies and activities of the service providers concerned in outsourcing should be consistent with and conducted alongside the critical operations management and dependency management for operational resilience. For other types of third party dependencies, an AI should consider the need for adopting similar risk management processes as detailed above having regard to the risks involved.

(e) **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. Please see AML-1 "Supervisory Approach on Anti-Money Laundering and Counter-Financing of Terrorism" for guidance on managing money laundering and terrorist financing risks.~~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.~~

(f) **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~~arise from such products.

(g) **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.

(h) **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".~~

(i) **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.

7.4.8 In circumstances where internal controls do not adequately address risks and exiting the risk is not a reasonable option, senior management can complement controls by seeking to transfer the risk to another party ~~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). The Board should determine the maximum loss exposure the AI is willing and has the financial capacity to assume, and should perform an annual review of the AI's risk and insurance management programme. While the specific insurance or risk transfer needs of an AI should be determined on an individual basis, consideration should always be given to applicable regulatory requirements.

8. Specific aspects of operational risk management

8.1 Change management

8.1.1 Change management should assess the evolution of the risks associated with the change initiatives of the AI (such as those referred to in para.7.4.7(a)) across time, from inception to termination (e.g. throughout the full life cycle of a product). The policies and procedures on change management should define the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update, and clearly allocate roles and responsibilities in accordance with the three lines of defence model, in particular:

(a) the first line of defence should perform operational risk and control assessments of new products, activities, processes and systems, including the identification and evaluation of the required change through the decision-making and planning phases

to the implementation and post-implementation review.

(b) the second line of defence (i.e. CORF) should challenge the operational risk and control assessments of first line of defence, as well as monitor the implementation of appropriate controls or remediation actions. CORF should cover all phases of this process. In addition, CORF should ensure that all relevant control groups (e.g. finance, compliance, legal, business, ICT, risk management) are involved as appropriate.

8.1.2 An AI should have policies and procedures for the review and approval of its change initiatives, covering:

(a) inherent risks including legal, ICT and model risks (especially when outsourcing is involved);

(b) changes to the AI's operational risk profile, appetite and tolerance, including changes to the risk of existing products or activities;

(c) necessary controls, risk management processes and risk mitigation strategies;

(d) residual risk;

(e) changes to relevant risk management thresholds or limits; and

(f) the procedures and metrics to assess, monitor and manage risks.

8.1.3 The review and approval process should include ensuring that appropriate investment has been made for human resources and technology infrastructure before changes are introduced. Changes should be monitored, during and after their implementation, to identify any material differences to the expected operational risk profile and manage any unexpected risks. Controls and procedures for identifying and assessing threats/vulnerabilities and operational risk should be assessed to ensure that they remain effective after a change to any underlying components of critical operations.

8.1.4 To facilitate the monitoring of changes, AIs should maintain a central record of their products and services (including outsourced functions or activities) to the extent possible.

8.1.5 AIs should also see section 4.3 of IC-1 "Risk Management Framework" for general guidance on risk management

relating to new products and services.

8.2 Information Communication and Technology

8.2.1 There are inherent risks and benefits in the application of ICT in the operations of AIs. While automated processes are less prone to error than manual processes, they introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes. In addition, the use of technology related products, activities, processes and delivery channels exposes an AI to operational risk and possibility of material financial loss. Consequently, AIs should have an integrated approach to ICT risk management under their ORMF. ICT risk management should ensure effective ICT performance and ICT security, contributing to an effective operating and control environment essential for achieving the AIs' strategic objectives. Sound ICT risk management reduces AIs' operational risk exposure to direct losses, legal claims, reputational damage, ICT disruption and misuse of technology in alignment with its risk appetite and tolerance statement.

8.2.2 To ensure the confidentiality, integrity and availability of data and system, the Board should regularly oversee the effectiveness of the AI's ICT risk management and senior management should routinely evaluate the design, implementation and effectiveness of the AI's ICT risk management. This requires regular alignment of the business, risk management and ICT strategies to ensure consistency with the AI's risk appetite and tolerance statement as well as with privacy and other applicable laws.

8.2.3 Effective ICT risk management should include the following processes:

(a) defining ICT risk;

(b) identifying the operations which are exposed to ICT risk and assessing the magnitude of the risk exposure (e.g. high, medium, low);

(c) implementing ICT risk mitigation measures consistent with the assessed risk level. Common measures include cybersecurity, response and recovery programmes, ICT change management processes, ICT incident management processes

(including relevant information transmission to users on a timely basis);

(d) monitoring the effectiveness of mitigation measures (including regular tests);

(e) regular reporting of ICT risks, controls and events to senior management.

8.2.4 ICT risk management together with complementing processes set by AIs should:

(a) be reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats (e.g. cyber) and evolving or new technologies;

(b) be regularly tested to identify gaps against stated risk tolerance objectives and facilitate improvement of the ICT risk identification, protection, detection and event management; and

(c) make use of actionable intelligence to continuously enhance their situational awareness of vulnerabilities to ICT systems, networks and applications and facilitate effective decision making in risk or change management.

8.2.5 AIs should develop approaches to ICT readiness for stressed scenarios from disruptive external events, such as the need to facilitate the implementation of wide-scale remote-access, rapid deployment of physical assets and/or significant expansion of bandwidth to support remote user connections and customer data protection. In this connection, AIs should ensure that:

(a) appropriate risk mitigation strategies are developed for potential risks associated with a disruption or compromise of ICT systems, networks and applications. AIs should evaluate whether the risks, taken together with these strategies, fall within their risk appetite and risk tolerance;

(b) well defined processes for the management of privileged users and application development are in place; and

(c) regular updates are made to ICT including cyber security in order to maintain an appropriate security posture.

8.2.6 Please also refer to TM-E-1 “Risk Management of E-

banking" and TM-G-1 "General Principles for Technology Risk Management" for relevant guidance.

8.3 Business continuity management and disaster recovery plan

8.3.1 All AIs should have in place formal contingency and business continuity plans (BCP)[21] 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.~~ The approval and subsequent reviews of the BCP by the Board should ensure that contingency strategies remain consistent with current operations, risks and threats and the AI's ORMF. A sound BCP requires the commitment of the first and second lines of defence to its design, strong involvement of senior management and business unit leaders in its implementation and regular review by the third line of defence.

8.3.2 Moreover, the BCP should be forward looking in the disruption scenarios, with relevant impact assessments and recovery procedures:

(a) the BCP should be based on scenario analyses of potential disruptions to the AI's operations. For the purpose of the analyses, all business units as well as critical service providers and major third parties (e.g. central banks, clearing house) of the AI should be covered, and critical business operations and key internal and external dependencies be identified and categorised;

(b) each scenario should be subject to a quantitative and qualitative impact assessment or business impact analysis with regard to its financial, operational, legal and reputational consequences; and

(c) disruption scenarios should be subject to thresholds or limits (such as maximum tolerable outage) for the activation of business continuity procedures. These procedures should address resumption aspects, set

[21] Business continuity planning should be consistent with and conducted alongside the same and the testing of critical operations as specified in the relevant guidance set out in OR-2.

recovery time objectives and recovery point objectives as well as communication guidelines for informing management, employees, regulatory authorities, customers, suppliers and where appropriate, civil authorities.

8.3.3 An AI should provide customised training and awareness programmes to its staff based on their specific roles to ensure that they can effectively execute contingency plans. Business continuity procedures should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met in the unlikely event of a severe business disruption. Where possible, an AI should participate in business continuity testing with key service providers. Results of formal testing and review activities should be reported to senior management and the Board.

8.3.4 Please also refer to TM-G-2 "Business Continuity Planning" for the sound practices which the HKMA expects AIs to ~~take~~adopt in their business continuity planning.

9. Disclosure

9.1 The regulatory disclosure requirements (including in relation to operational risk exposures and operational risk management) that AIs are required to comply with are specified in the Banking (Disclosure) Rules (Cap 155M). These Rules are supplemented by interpretative guidance contained in CA-D-1 "Guideline on the Application of the Banking (Disclosure) Rules".

9.2 Outlined below are a few general principles that AIs are expected to follow in particular to enable its stakeholders to assess its approach to operational risk management and its operational risk exposure:

(a) an AI should publicly disclose information on its operational risk management. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of the AI's operations, and should take into account evolving industry practices;

(b) an AI should also disclose relevant operational risk exposure information to its stakeholders (including significant operational loss events[22]) while not creating operational risk through this disclosure (e.g. description of unaddressed control vulnerabilities). An AI should disclose its ORMF in a

[22] The recommendation to disclose significant operational loss events does not include disclosure of confidential and proprietary information, including information about legal reserves.

manner that allows stakeholders to determine whether the AI identifies, assesses, monitors and controls/mitigates operational risk effectively; and

(c) an AI should have a formal disclosure policy that is subject to regular and independent review and approval by the senior management and the Board. The policy should set out the AIs' approach for determining what operational risk disclosures they will make and the internal controls over the disclosure process. In addition, AIs should implement a process for assessing the appropriateness of their disclosures and disclosure policy.

Annex: Detailed loss event type classification

Event-type category (Level 1)	Definition	Categories (Level 2)	Activity examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party	Unauthorised activity	• Transactions not reported (intentional) • Transaction type unauthorised (with monetary loss) • Mismarking of position (intentional)
		Theft and fraud	• Fraud / credit fraud / worthless deposits • Theft / extortion / embezzlement / robbery • Misappropriation of assets • Malicious destruction of assets • Forgery • Check kiting • Smuggling • Account takeover / impersonation etc • Tax non-compliance / evasion (wilful) • Bribes / kickbacks • Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and fraud	• Theft / robbery • Forgery • Check kiting
		Systems security	• Hacking damage • Theft of information (with monetary loss)

Event-type category (Level 1)	Definition	Categories (Level 2)	Activity examples (Level 3)
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee relations	• Compensation, benefit, termination issues • Organised labour activity
		Safe environment	• General liability (slip and fall etc) • Employee health and safety rules events • Workers compensation
		Diversity and discrimination	• All discrimination types
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product	Suitability, disclosure and fiduciary	• Fiduciary breaches / guideline violations • Suitability / disclosure issues (know-your-customer etc) • Retail customer disclosure violations • Breach of privacy • Aggressive sales • Account churning • Misuse of confidential information • Lender liability
		Improper business or market practices	• Antitrust • Improper trade / market practices • Market manipulation • Insider trading (on firm's account) • Unlicensed activity • Money laundering
		Product flaws	• Product defects (unauthorised etc) • Model errors
		Selection, sponsorship and exposure	• Failure to investigate client per guidelines • Exceeding client exposure limits

Event-type category (Level 1)	Definition	Categories (Level 2)	Activity examples (Level 3)
		Advisory activities	• Disputes over performance of advisory activities
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events	Disasters and other events	• Natural disaster losses • Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	• Hardware • Software • Telecommunications • Utility outage / disruptions
Execution, delivery and process management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction capture, execution and maintenance	• Miscommunication • Data entry, maintenance or loading error • Missed deadline or responsibility • Model / system misoperation • Accounting error / entity attribution error • Other task misperformance • Delivery failure • Collateral management failure • Reference data maintenance
		Monitoring and reporting	• Failed mandatory reporting obligation • Inaccurate external report (loss incurred)
		Customer intake and documentation	• Client permissions / disclaimers missing • Legal documents missing / incomplete
		Customer / client account	• Unapproved access given to accounts

Event-type category (Level 1)	Definition	Categories (Level 2)	Activity examples (Level 3)
		management	• Incorrect client records (loss incurred) • Negligent loss or damage of client assets
		Trade counterparties	• Non-client counterparty misperformance • Miscellaneous non-client counterparty disputes
		Vendors and suppliers	• Outsourcing • Vendor disputes