HONG KONG MONETARY AUTHORITY 香港金融管理局		
Supervisory Policy Manual		
RR-1	**Reputation Risk Management**	V.1 – 17.12.08

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' reputation risk, and to provide guidance to AIs on the key elements of effective reputation risk management

Classification

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

Previous guidelines superseded

This is a new guideline

Application

To all AIs

Structure

1. Introduction
   - 1.1 Terminology
   - 1.2 Background
   - 1.3 Scope
   - 1.4 Related legal obligations
   - 1.5 Implementation
2. Supervisory approach to reputation risk
   - 2.1 Supervisory objectives
   - 2.2 Supervisory process
   - 2.3 Supervisory assessment
3. Sources of reputation risk
   - 3.1 Overview

1. Introduction

1.1 Terminology

1.1.1 This subsection sets out the meanings of reputation risk and other related terms used in this module.

1.1.2 "Reputation" means a collection of the perception, opinions and beliefs that an AI's stakeholders have in respect of the AI, based on their experience with, or expectations of, the AI.

1.1.3 "Reputation event" includes any action, incident or circumstance in relation to an AI which induces, or is likely to induce, reputation risk for the AI. For example, such an event may arise from market rumours, severe regulatory sanctions, or heavy financial losses. Some of these events, if not acted upon swiftly and effectively, may turn into a full-blown crisis (e.g. a bank run).

1.1.4 "Reputation risk" means the risk that an AI's reputation is damaged by one or more than one reputation event, as reflected from negative publicity about the AI's business practices, conduct or financial condition. Such negative publicity, whether true or not, may impair public confidence in the AI, result in costly litigation, or lead to a decline in its customer base, business or revenue.

1.1.5 "Reputation risk management process" means the risk management process adopted by an AI to identify, assess, control, monitor and report reputation risk.

1.1.6 "Stakeholders" mean those groups of individuals or organisations that (i) are involved or interested in the affairs of an AI, or (ii) can exert an influence over, or are affected by, the AI and its activities.[1]

1.2 Background

1.2.1 Reputation plays a key role in determining whether an AI has a sustainable future for its business. Where an AI has established a good reputation, it helps strengthen the trust and confidence of the AI's major stakeholders, which serves

[1] Broadly speaking, stakeholders may include an AI's shareholders, investors, employees, customers, counterparties, business partners, service providers and other interested parties such as governments, regulators, rating agencies, analysts, non-governmental organisations, pressure groups, the media and those communities in which the AI operates.

to bolster its safety and soundness, competitiveness and business value. A good reputation may also increase the AI's chance of overcoming a market crisis when it occurs. If, however, an AI's reputation has been badly damaged, thereby undermining public confidence in the AI, its business prospects and survival could be at stake. Managing reputation risk (or, more precisely, those risks affecting reputation) and dealing with its underlying problems and effects therefore warrant AIs' special attention and priority.

1.2.2 Typically, reputation could be damaged by an AI's failure to properly manage the risks it faces (such as credit, strategic, operational or other material risks) as well as some external factors that are beyond its control (e.g. market rumours). Such damage may lead to serious consequences with immediate or long term implications. For example, if the source of reputation risk is from staff fraud resulting in substantial losses, the potential consequences may involve criminal / regulatory investigations, falling share price, ratings downgrade, loss of business, depletion of earnings and capital, or liquidity problems.

1.2.3 Reputation risk management is essentially concerned with protecting an AI from potential threats to its reputation (e.g. by dealing with those threats proactively) and, should there be a reputation event, minimising the effects of such an event. The ultimate aim is to avert the likelihood of any crisis. Nevertheless, managing reputation risk poses particular challenges for AIs.

1.2.4 Reputation, being largely based on people's perception and expectations, is intangible in nature and thus cannot be easily analysed or quantified. A lot of persistent effort is required to maintain reputation. While a good reputation may take many years to build up, it can be tarnished instantly by, for example, some tactless remarks from a director or an operational blunder committed by a few employees. Indeed, reputation is subject to a whole host of risk drivers (see section 3 for more details), and anyone within an AI (or even anyone within its major service providers) may potentially affect its reputation.

1.2.5 Moreover, it is worth noting that an AI's reputation depends not only on winning the trust and confidence of the AI's shareholders and customers, but also on procuring the support of other major stakeholders who can influence its ability to run a successful business (see para. 1.1.6). Thus, a

key responsibility of the AI is to identify its major stakeholder groups for the purposes of managing reputation risk and consider how their needs and expectations can be satisfied (see para. 6.3.6).

1.2.6 Respect for, and commitment to, high standards of business conduct and integrity, among other things, are fundamental to maintaining a sustainable reputation. Any breach of or compromise on ethical standards and rules of conduct (e.g. engaging in improper selling practices) runs the risk of impairing stakeholder confidence and may have serious business and regulatory consequences. Reputation can also be damaged by association, even unknowingly, with unethical or corrupt customers (e.g. those engaging in money laundering or bribery activities).

1.2.7 AIs should be aware of increasing expectations from the public for them to take up social responsibilities and operate in an environmentally responsible manner. These include, for example, taking care of the special needs of the elderly or handicapped customers when formulating business strategies and adopting green policies to reduce wastage and pollution. Corporate social responsibility has thus become an issue that may have an impact on reputation as well.

1.2.8 Despite the various challenges mentioned above, there is growing recognition that managing reputation is crucial for business success and sustainability. It is therefore in AIs' interests to actively manage reputation risk, which includes identifying and assessing threats to their reputation and exploring opportunities for enhancing it. This module contains relevant guidance that AIs could adopt in their risk management processes.

1.3 Scope

1.3.1 The HKMA expects every AI to establish an effective process for managing reputation risk that is appropriate for the size and complexity of its operations. This is consistent with Principle 7 of the revised "Core Principles for Effective Banking Supervision" issued by the Basel Committee whereby banks are required to have in place a comprehensive risk

management process in respect of all material risks (including reputation risk)[2].

1.3.2 Recognising that reputation risk management is still at an early stage of development, the HKMA does not propose to prescribe any specific methodology or framework for managing such risk. This module focuses mainly on –

- elaborating on the HKMA's approach to supervising reputation risk;
- drawing AIs' attention to various sources of reputation risk;
- providing them with guidance on the key elements of reputation risk management; and
- promoting their adoption of a formalised and structured approach to managing reputation risk.

1.3.3 The HKMA will continue to monitor international developments on reputation risk management practices. This module may therefore be subject to revision and additional guidance as internationally accepted standards and practices on reputation risk management emerge over time.

1.4 Related legal obligations

1.4.1 While this module does not have the force of law, the adequacy of an AI's reputation risk management, or the occurrence of any reputation event (which may relate to the conduct of specific management or staff members), may have a bearing on the HKMA's assessment of the AI's ongoing compliance with the following authorization criteria:

- Paras. 4 and 5 of the Seventh Schedule to the Banking Ordinance requiring every director, chief executive, executive officer or controller[3] of an AI to be a fit and proper person to hold the particular position which he holds or is to hold. As the probity of these persons is very important to the AI's reputation, it is essential that these persons are of high integrity. In considering whether they fulfil this criterion, the HKMA will pay particular attention to

[2] The relevant information is contained in the Basel Committee paper on "Core Principles Methodology" updated in October 2006.

[3] The controller referred to here is in respect of a locally incorporated AI.

such factors as their reputation, character, reliability, financial status, honesty, and their record of compliance with statutory and non-statutory codes and requirements, in addition to other relevant factors;

- Para. 5A of the Seventh Schedule to the Banking Ordinance requiring AIs to have adequate systems of control to ensure the fitness and propriety of their senior executives, who are referred to as "managers" in the Ordinance. In considering whether an AI fulfils this criterion, the HKMA will take into account, among other things, the factors set out in CG-2 "Systems of Controls for the Appointment of Managers";
- Para. 10 of the Seventh Schedule to the Banking Ordinance requiring AIs to maintain adequate accounting systems and systems of control. These are essential for ensuring the prudent and efficient running of the business, safeguarding the assets of the AI, minimising the risk of fraud, monitoring the risks to which the AI is exposed and complying with legislative and regulatory requirements; and
- Para. 12 of the Seventh Schedule to the Banking Ordinance requiring AIs to conduct their business (including banking and non-banking business) with integrity, prudence and professional competence and in a manner which is not detrimental to the interests of deposits or potential depositors. In assessing compliance with this criterion, the HKMA will consider, among other things, AIs' observance of high ethical standards in carrying on their business, their general reputation and standing in the financial community, and their general competence as demonstrated, for example, by their resistance to internal and external fraud and avoidance of operational errors. Any criminal offence, breach of law and regulations, and failure to comply with recognised standards of conduct[4], and any other act or behaviour reflecting dishonesty, incompetence or malpractice may call into question the fulfilment of this criterion.

[4] The recognised standards of conduct include those embodied in various codes of conduct, particularly those relating to banking practices, regulated activities specified under the Securities and Futures Ordinance, the prevention of money laundering, customer complaints and debt collection agencies.

1.4.2 The HKMA would expect AIs (including branches of foreign-owned banks) to notify it promptly of any reputation event which, in their view, may have a significant impact on their business or reputation, or is likely to lead to a crisis, notwithstanding that there may not be a statutory requirement to do so. Where appropriate, AIs should also keep their home or host supervisors informed of the situation.

1.4.3 In addition, AIs should be mindful of, and ensure compliance with, any relevant reporting obligations under other laws, rules and regulations such as the Securities and Futures Ordinance and the Rules Governing the Listing of Securities on The Stock Exchange of Hong Kong Limited.

1.5 Implementation

1.5.1 AIs should ensure that their reputation risk management is commensurate with the nature, size and complexity of their business, appropriate for their individual circumstances and needs, and consistent with the risk management guidance laid down in this module.

1.5.2 AIs should incorporate all relevant guidance regarding reputation risk management into their risk management processes as soon as practicable, but not later than 12 months of the issue date of this module or such further period as may be agreed with the HKMA.[5] The HKMA will monitor AIs' progress in enhancing reputation risk management and take into account the progress achieved in determining its supervisory priorities.

1.5.3 Where AIs have adopted an approach to reputation risk management which may not be in line with the guidance set out in this module, they should provide adequate justification for the approach taken and be able to demonstrate to the HKMA's satisfaction that alternative measures are in place to control or mitigate reputation risk.

[5] This grace period is only applicable to existing AIs at the issue date of the module.

2. Supervisory approach to reputation risk

2.1 Supervisory objectives

2.1.1 Reputation risk is one of the eight inherent risks[6] which the HKMA has identified as risks to be assessed under its risk-based supervisory process (see SA-1 "Risk-based Supervisory Approach" for more details). AIs are required to establish a sound and effective system to manage each of these risks.

2.1.2 The main objectives of the HKMA's risk-based supervisory approach in respect of reputation risk are to assess –

- the level and trend of AIs' reputation risk;
- the adequacy and effectiveness of their reputation risk management; and
- their reputation risk profile.

2.1.3 In the case of locally incorporated AIs, the adequacy of their capital relative to the level of their reputation risk and the soundness of their reputation risk management will also be assessed as part of the supervisory review process ("SRP") (see CA-G-5 "Supervisory Review Process" for more details).

2.1.4 Results of the HKMA's assessment under paras. 2.1.2 and 2.1.3, together with the assessment results for other inherent risks, will be used for determining the overall risk profile of, and the HKMA's supervisory priorities in respect of, AIs and, in the case of locally incorporated AIs, their minimum capital adequacy ratio.

2.2 Supervisory process

2.2.1 Under its risk-based supervisory approach, the HKMA exercises continuous supervision of AIs' reputation risk through a combination of risk-focused on-site examinations, off-site reviews and prudential meetings.

2.2.2 The HKMA monitors the reputation risk profile of AIs (including changes in their level and direction of reputation risk) during off-site reviews and prudential meetings, and evaluates the effectiveness of their reputation risk

[6] The other seven inherent risks are credit, market, interest rate, liquidity, operational, strategic and legal risks.

management during on-site examinations. In the case of locally incorporated AIs, the HKMA will additionally review how they deal with reputation risk under their capital adequacy assessment process, and evaluate whether this process is effective in assessing their capital adequacy in relation to their risk profile (taking into account reputation risk), as part of the SRP.

2.2.3 In evaluating AIs' reputation risk management, the HKMA will adopt a system-based approach that puts the main focus on the policies, systems, processes and controls established by AIs. The HKMA will also have regard to the effectiveness of their approach to managing reputation events that have taken place. To facilitate its assessment, the HKMA will obtain relevant information from AIs which may include, but is not limited to, the following:

- the strategies, policies, codes of conduct, guidelines and procedures relevant to reputation risk management;
- documentary evidence reflecting AIs' risk identification, assessment, control, monitoring and reporting processes (including early warning systems), as well as other available measures for mitigating reputation risk;
- management reports submitted to the Board, specialised committees and senior management to facilitate reputation risk management;
- minutes of Board or committee meetings and discussion papers with regard to reputation risk management;
- results of any independent review or audit relating to reputation risk management;
- communication arrangements for media relations and external reporting; and
- historical records of reputation events, if any, and how they were managed.

2.2.4 The HKMA will also hold periodic discussions with AIs' Board and senior management (e.g. during annual Board or prudential meetings) to gain deeper insight into their overall reputation risk management, including any comments on reputation issues or risk management weaknesses identified.

2.2.5 The HKMA will adopt a proportionate approach in relation to application of the risk management guidance set out in this

module to AIs of varying size and complexity. For example, AIs with small, simple operations will not be expected to have an approach to reputation risk management as elaborate as those with more complex operations. However, they should, at a minimum, be able to demonstrate that their reputation risk management covers the key elements set out in section 4, although the procedures and documentation involved can be more simplified.

2.2.6 In the case of AIs which are branches of foreign-owned banks, the HKMA will focus its assessment of reputation risk management on those matters relevant to the branch operations. In particular, the HKMA will assess whether local branch management has maintained adequate systems and controls for managing reputation risk and handling reputation events in Hong Kong. The HKMA will have regard to any group-wide policies on reputation risk management that may be applicable to the branch (and whether such policies have been tailored to suit local circumstances) as well as any relevant information or comments that may be obtained from its home supervisor. Where necessary, the HKMA may request local branch management to provide relevant information regarding the branch's reputation risk management for its assessment. The branch may discuss with the HKMA if it has any problem in satisfying the HKMA's information request.

2.2.7 If deficiencies are found in an AI's reputation risk management, the HKMA will enter into discussions with the AI and seek prompt remedial action. Depending on the circumstances of each case, the HKMA may require the AI to take actions to mitigate specific concerns (e.g. some impending threats to its reputation).

2.2.8 Under §59(2) of the Banking Ordinance, the MA has the power to require an AI, after consultation with the AI, to provide an auditors' report on such matters as he may specify for the performance of his functions under the Ordinance. The MA may exercise this power to commission an auditors' report, for example, when he considers that an independent review of the AI's reputation risk management, or an independent investigation into some reputation issues, is warranted.

2.3 Supervisory assessment

2.3.1 This subsection describes the key factors that will be considered by the HKMA in assessing –

- the level and trend of AIs' reputation risk;
- the adequacy and effectiveness of their reputation risk management; and
- their reputation risk profile.

2.3.2 The HKMA will use a combination of techniques, such as qualitative analysis, peer group comparison and supervisory judgement, in its assessment of reputation risk.

Level and trend of AIs' reputation risk

2.3.3 The major factors that the HKMA will take into account in assessing the level and trend of an AI's reputation risk are listed below. These are not necessarily all-inclusive, but will serve as a guide for assessment purposes –

- the market or public perception of the financial strength of the AI's major shareholders, its management and financial stability, and the prudence of its business practices;
- management's willingness and ability to adjust, where necessary, the AI's strategies to enhance its reputation and standing (e.g. in response to changes in market perception, rules and regulations, or legal barriers);
- the AI's history of formulating business strategies and making commercial decisions that affect its financial position, business conduct and reputation, including those that reflect on the fairness and integrity of its business dealings (e.g. in relation to the provision of banking services, charging of fees, etc.);
- the AI's history of, and plans for, analysing risk in new products and services, developing relevant policies and conducting due diligence;
- the nature and volume of customer complaints and management's willingness and ability to respond to those complaints;
- management's ability to handle any scandal or negative publicity to minimise damage to the AI's reputation;

- the existence of highly visible or conspicuous litigation (and historical losses arising from such litigation);
- the existence of appropriate fiduciary or other liability insurance to mitigate potential losses arising from litigation or claims; and
- the AI's history with respect to conduct of business practices and compliance with laws and regulations, and management's willingness and ability to address concerns uncovered in internal or regulatory reviews.

2.3.4 For AIs which are subsidiaries within a banking group (local or foreign) or are branches of foreign-owned banks, the HKMA will additionally consider whether the financial position, reputation or conduct of the parent bank or head office, or any other member of the group could undermine confidence in the AI through "contagion". The risk of contagion is not confined to financial weaknesses. Adverse publicity about illegal or unethical conduct by those entities may also damage the AI's reputation.

2.3.5 The HKMA will adopt a forward-looking approach and take into account any significant changes (either arising from institutional or external conditions) in the past year that may affect the direction of an AI's reputation risk in the coming year (i.e. whether the level of reputation risk is "increasing", "stable" or "decreasing"). The public perception and market standing of the AI and its peers will also be compared.

Reputation risk management

2.3.6 In assessing the adequacy and effectiveness of an AI's reputation risk management, the HKMA will have regard to the following factors:

- the appropriateness of the AI's reputation risk management relative to its nature, size and complexity of business;
- the overall effectiveness of the AI's reputation risk management, taking into account the extent to which the AI has adopted risk management practices recommended in this module or other comparable practices that serve similar purposes;

- the adequacy of the AI's corporate governance in respect of reputation risk (see section 5 for more guidance), including –
  - the AI's obligations and accountability to major stakeholders;
  - the AI's willingness and ability to adapt to changing circumstances, and to recalibrate its vision, values, strategic goals and supporting policies to keep pace with evolving stakeholder requirements and expectations;
  - the AI's willingness and ability to create a corporate culture which upholds integrity and responsible and ethical behaviour as the norm within the AI;
  - the level of participation and involvement of the Board and senior management, and their knowledge and experience, in reputation risk management; and
  - the level of oversight exercised by independent non-executive directors over the AI's business and management performance;
- the effectiveness of the AI's reputation risk management process (see section 6 for more guidance), including whether –
  - the risk management process is capable of detecting and responding swiftly to new and emerging threats to reputation, monitoring the changing status of risks, providing early warning of potential problems to enable prompt corrective actions to be taken, and providing credible assurance that the risks affecting reputation are under control; and
  - all relevant individuals have taken responsibility for managing the risks affecting reputation in their own area and for identifying and acting on such risks affecting the business as a whole; and
- the robustness and comprehensiveness of the AI's approach to managing reputation events (see section 7 for more guidance), including –
  - the ability to recognise any direct threat to reputation early and prepare for it; and

- the delivery of an effective action plan to limit damage to reputation and expedite recovery.

Reputation risk profile

2.3.7 Based on the above assessment results, the HKMA will decide upon an AI's reputation risk profile (categorised as "low", "moderate" or "high"). **Annex A** provides a summary of major characteristics under each of these risk categories.

2.3.8 Where appropriate, the HKMA will discuss with the AI concerned the assessment results on reputation risk, and any issues or concerns arising therefrom.

3. Sources of reputation risk

3.1 Overview

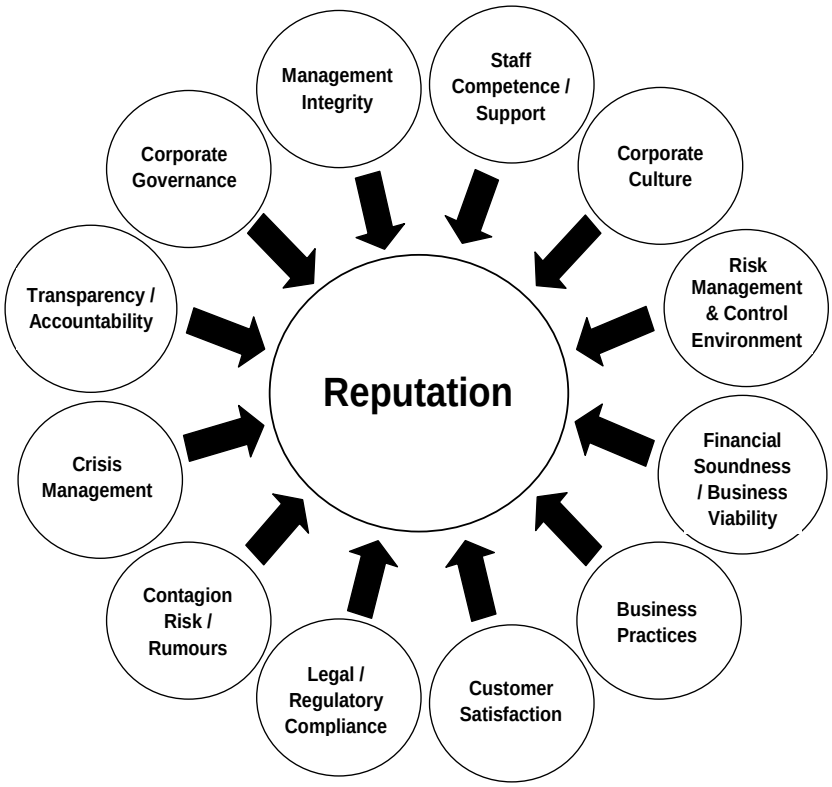
3.1.1 Reputation can be at risk in so many varied ways that it is essential for AIs to understand how different sources of reputation risk will impact on them such that appropriate systems and controls can be used to manage the risks involved. Subsection 3.2 sets out various key drivers of reputation, which could help AIs in identifying and categorising major sources of reputation risk applicable to them.

3.1.2 AIs could also analyse what basic qualities (e.g. integrity, competence, efficiency, reliability, service quality, etc.) are expected of them from their major stakeholders and what special attributes (e.g. strong credit ratings) they possess compared to their peers. Any risk that undermines such qualities or attributes will pose threats to their reputation.

3.2 Key drivers of reputation

3.2.1 **Diagram 1** below provides some key drivers of reputation relevant to AIs. It should be noted that many of the reputation drivers are inter-related, represent common factors applicable to AIs (and hence are not necessarily all-inclusive), and relate fundamentally to how well an AI has managed its business and controlled its material risks.

Diagram 1 : Key drivers of reputation



3.2.2 The above-mentioned reputation drivers are further described in **Annex B**, which explains how each of these drivers may affect reputation risk and provides some relevant considerations for managing their effects on reputation.

3.2.3 In identifying potential threats to reputation, AIs should assess whether there are any "weak spots" in respect of the reputation drivers that they should attend to proactively. See subsection 6.3 for more details about risk identification, assessment and control.

4. Reputation risk management

4.1 Overview

4.1.1 AIs should adopt an approach to reputation risk management that fits their own risk profile and level of sophistication, and that enables the risks affecting reputation to be consistently and comprehensively identified, assessed, controlled, monitored, and reported.

4.1.2 There is no prescribed approach to reputation risk management. The risk management guidance set out in this module therefore mainly serves to illustrate the key elements of reputation risk management that the HKMA expects to see in AIs' risk management processes. AIs may adopt other alternative approaches provided that they achieve similar risk management purposes.

4.2 Key elements

4.2.1 Reputation risk management has three main building blocks:

- good corporate governance;
- effective reputation risk management process; and
- adequate management of reputation events.

4.2.2 Good corporate governance forms the foundation of effective reputation risk management (see section 5 for more details), and provides a framework for –

- guiding AIs' conduct and actions in achieving their vision, values, goals and strategies as well as meeting stakeholder requirements and expectations; and
- ensuring robust oversight of their conduct and actions.

4.2.3 Central to reputation risk management is an effective process for managing the risks affecting reputation (see section 6 for more details). A major objective of this process is to prevent any perceived risks from developing into direct threats to AIs' reputation. Some basic elements are described below:

- Policies, codes of conduct, guidelines and procedures which guide staff behaviour and conduct, and set boundaries for staff actions, in particular the boundaries for unacceptable practices;
- Risk identification, assessment and control which provide a systematic process for identifying and assessing the risks affecting reputation, including the setting of appropriate response actions to control the risks;
- Risk monitoring and reporting which ensure that –
  - the progress of carrying out agreed response plans is adequately monitored;
  - the changing status of the risks concerned is regularly reviewed; and

- early warning systems are in place for identifying emerging threats and ensuring that prompt corrective actions are taken to address those threats;

- Communications and disclosure which enable meaningful, transparent and timely information to be provided to stakeholders to better their understanding of the AI's performance and future prospects, and to retain their confidence; and

- Independent reviews and audits which give assurance that the risks affecting reputation have been adequately understood and properly controlled throughout the AI.

4.2.4 As reputation events may still occur despite stringent risk control measures, it is pertinent for AIs to develop a systematic and comprehensive approach to managing reputation events so that AIs' management can, as soon as possible, be informed of and prepared for such events and be able to take proper measures to restore the institution's reputation and minimise any damage so caused (see section 7 for more details). The effectiveness of this approach would help reduce the chance of having to deal with a full-blown crisis.

5. Corporate governance

5.1 Overview

5.1.1 Successful reputation risk management would not be possible without team effort. Good corporate governance helps ensure that everyone within an AI makes an effort in moulding and upholding its reputation. This can be achieved by implementing a governance infrastructure (see subsection 5.2) and adopting governance practices (see subsection 5.3) that meet stakeholders' expectations. Major roles played by different parties within an AI on reputation risk management are highlighted in subsection 5.4.

5.1.2 The HKMA would expect AIs incorporated in Hong Kong to comply with the minimum standards set out in CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions". Where necessary, they may consider forming one or more than one specialised committee to assist the Board in corporate governance matters, including overseeing the overall reputation risk management process, leading the

process for Board appointments, or recommending remuneration and compensation for directors and management. Ideally, the specialised committee(s) should consist of a majority of independent directors[7] so as to avoid management dominance within the committee(s).

5.1.3 In the case of AIs which are branches of foreign-owned banks, the HKMA would expect the branches to be governed by their head office's corporate governance infrastructure and practices. Where appropriate, the HKMA may request the foreign bank's home supervisor to provide information and comments in respect of the bank's corporate governance, and will take account of such information and comments in its supervisory assessment of the branch (e.g. the extent to which the branch's operations may be affected by any corporate governance issues at the head office level).

5.2 Governance infrastructure

5.2.1 A sound governance infrastructure should have the following general attributes:

- having the right people with the right balance of skills and experience on the Board, and putting in place suitable checks and balances to ensure that no single individual can influence Board decisions;
- including a robust framework for succession planning in the Board's processes so as to ensure that the business can continue to function effectively, even when there is major management or staff turnover; and
- enabling business and management performance to be closely overseen by independent directors. To facilitate this, AIs should ensure that independent directors have sufficient, accurate and timely information for making sound judgement and effective contributions.

5.2.2 In addition, AIs are expected to adopt a governance approach which should, among other things, set out clear governance objectives and expectations on reputation risk management as well as the authorities and responsibilities of all parties

[7] As defined in CG-1 "Corporate Governance of Locally Incorporated Authorized Institutions", an independent director is a non-executive director who is not involved in the AI's management and is free from any business or other relationship which could materially affect his independent judgement in relation to the AI's affairs.

engaged in the risk management process. Such authorities and responsibilities should be adequately disseminated to all relevant parties, and there should be an effective process for monitoring their performance and prompting management to take early corrective actions before any damage to reputation is caused.

5.3 Governance practices

5.3.1 Some general requirements and expectations that stakeholders have on governance practices are illustrated below. These are not necessarily all-inclusive, but will serve as a guide for AIs to develop best governance practices:

- setting clear and unambiguous vision, values, goals and strategies and ensuring that they are transparent and consistent with the requirements and expectations of an AI's major stakeholders;
- developing appropriate policies, codes of conduct, guidelines and procedures to support the implementation of the AI's vision, values, goals and strategies;
- creating an open and empowering corporate culture to encourage responsible and ethical behaviour, and to support the achievement of business objectives and effective risk management;
- building up a strong, stable management team which needs to be honest, competent, responsible, accountable and responsive to stakeholders;
- raising the risk awareness of employees and providing employees with adequate training to enable them to discharge their responsibilities on reputation risk management competently;
- setting up effective systems and controls to manage and control all material risks (including reputation risk) faced by the AI and to monitor compliance with all applicable laws, regulatory standards, best practices and internal guidelines; and
- having adequate policies and procedures in place to ensure that all disclosures to stakeholders are clear, accurate, complete, relevant, consistent and timely, and guided by the principles of ethics, integrity and transparency.

5.4 Risk management responsibilities

5.4.1 Everyone in an AI has a role to play in managing reputation risk. The following sets out some relevant responsibilities for different parties:

- The Board plays a crucial role in setting the right tone from the top so that appropriate emphasis can be given to managing material risks (including reputation risk);
- Senior management implements the Board's risk management policies and ensures that relevant control systems work as intended;
- Other levels of management play a part in –
  - promoting staff awareness of reputation risk in their respective business, operation or function (in particular those that interact directly with major stakeholder groups);
  - identifying key risks (e.g. strategic and operational risks) that could significantly affect the AI's reputation or business and bring them to senior management's attention;
  - being alert to early warning indicators of potential problems or threats to reputation;
  - ensuring that reputation risk is properly managed, with no major risks affecting reputation being inadvertently excluded *(for dedicated risk management personnel)*;
- All other employees can help to uphold the AI's reputation through their behaviour, remarks and actions which may influence stakeholders' perception of the AI;
- Internal audit can provide independent assurance of the adequacy of risk management processes and the effectiveness of actions taken to control individual risks affecting reputation; and
- Public relations unit (or its equivalent) can help promote effective external communications, especially in the handling of reputation events, and ensure that the reputation perspective is adequately considered in the AI's risk management processes.

5.4.2 As AIs' reputation could also be damaged by substandard service quality, improper acts, or lax controls of some key service providers (e.g. outsourced telephone banking operations, IT support, debt collection services, etc.), they should closely monitor the performance of these providers (including service commitments and undertakings, or adherence to relevant rules of conduct) and ensure that continued business relationships with these providers will not jeopardise reputation. See SA-2 "Outsourcing" for more guidance.

6. Reputation risk management process

6.1 Overview

6.1.1 The key elements of an effective reputation risk management process should include:

- policies, codes of conduct, guidelines and procedures;
- risk identification, assessment and control;
- risk monitoring and reporting (including early warning systems);
- communications and disclosure; and
- independent reviews and audits.

6.1.2 AIs should designate appropriate personnel (e.g. from risk management or other control units) to be responsible for designing, implementing, coordinating, and monitoring the reputation risk management process.

6.1.3 An AI's reputation risk management process may be standalone, centralised or integrated with other risk management processes, depending on how the process will fit into the AI's existing management structure and the nature and complexity of its operations. Regardless of the approach adopted, there should be processes in place that enable senior management to monitor reputation risk within and across different businesses and functions of the organisation such that any material issues or developments can be acted upon quickly and reported to the Board as appropriate.

6.2 Policies, codes of conduct, guidelines and procedures

6.2.1 AIs should have in place appropriate policies, codes of conduct, guidelines and procedures for managing the risks

affecting reputation not only to achieve business goals in accordance with their vision and values, but also to guide the behaviour and acts of staff. In the case of other related parties (e.g. major service providers and joint venture partners), they should be made aware of AIs' expectations on their business conduct and servicing standards, and there should be adequate procedures and controls to monitor their performance.

6.2.2 As guiding documents, the policies, codes of conduct and guidelines should clearly define expected, undesirable or unlawful (e.g. money laundering and bribery) practices, set out the boundaries of acceptable risks for different business activities and areas of operations, take into account the potential impact of any proposed activities or operations on customers and the general public, and be adequately disseminated to all relevant parties.

6.2.3 In addition, there should be a process to formally approve, review and update the guiding documents, and the approving authority and procedures should be clearly defined and documented. Normally, the policies and codes of conduct are approved by the Board or its delegated committee while the supporting guidelines are approved by management designated for the purpose. All guiding documents should be periodically reviewed and updated to ensure their appropriateness.

6.3 Risk identification, assessment and control

General

6.3.1 AIs should adopt a systematic approach to identifying, assessing and controlling any risk or potential threat that may adversely affect their reputation, having regard to the guidance set out in this subsection. Whatever approach is employed, it should be relevant to their business and risk profile, and tailored to their individual circumstances and needs.

6.3.2 AIs should adequately document the results of their risk identification and assessment, as well as the decisions and action plans to control the risks concerned. **Annex C** provides an example of how AIs may make use of a risk register for documenting the results of these processes.

Risk identification

6.3.3 AIs should develop a process for identifying reputation risk that –

- clearly defines the types of risk they would expect to capture and the areas of their focus in their risk management policy;
- establishes the key sources of reputation risk they are exposed to based on their individual circumstances (see section 3 for more guidance). These sources of risk may be classified by risk category, business activity or area of operations;
- describes the risks identified in terms of the nature of risk and the potential consequences that the risks may bring to their reputation;
- takes into account any risks arising from new business projects which may affect reputation; and
- has procedures to ensure that the risks identified are subject to ongoing review and no major risk areas are ignored or missed.

6.3.4 AIs should involve all relevant staff (e.g. those representing major departments, business or functional units) in the risk identification process using such techniques as are appropriate to the circumstances. These may be in the form of interviews, questionnaires, risk identification workshops, or self-assessments.

6.3.5 AIs should also refer to other relevant information for risk identification purposes. Such information may, for example, be sourced from media reports, stakeholder analysis reports (see below), internal audit and compliance reports, management exception reports, or other early warning indicators (see also subsection 6.5).

6.3.6 Stakeholder analysis constitutes an important part of an AI's risk identification process, given that reputation is largely about stakeholders' trust and confidence. Key steps include –

- identifying the core stakeholder groups which are most influential in terms of affecting the AI's business and reputation;

- understanding their demands and expectations, and identifying any issues or threats affecting their perception of the AI and what possible actions they may take if their concerns are not addressed[8]; and
- feeding any emerging issues or threats into the risk identification process.

6.3.7 As stakeholders' expectations and concerns will change over time, AIs should conduct regular stakeholder monitoring to ensure that no new issues or threats are overlooked.

Risk assessment

6.3.8 AIs should have procedures for assessing and prioritising the risks identified in terms of analysing the likelihood of the risk materialising into a reputation event (or a direct threat to reputation) and the impact of the risk on their business, financial strength and reputation, etc.

6.3.9 To facilitate assessment of the likelihood and impact of the risks identified, AIs may employ various techniques and tools, such as –

- Control assessment – this involves assessing the likelihood of the risk materialising by analysing the root causes of the risk, existing controls to manage the risk, and the effectiveness of such controls. AIs may also take into account other available information (e.g. internal or external audit reports) that provides independent assessment of how well the risk is being controlled;
- Stakeholders' impact assessment – this involves assessing the impact of the risk by identifying which stakeholder groups are most concerned with the risk, deciding whether these groups have a critical influence on AIs, and anticipating the likely impact on them if these stakeholders react adversely to the risk; and
- Stress-testing – this technique is useful for identifying events or changes that pose threats to AIs, and can help develop different sets of circumstances which could

[8] If there are any conflicts in the interests of different stakeholder groups which pose problems to satisfying the groups' expectations, AIs should decide carefully how to deal with such situations and strike an appropriate balance after taking into account all potential consequences arising from their decisions.

potentially spark a crisis. AIs can make use of this technique to assess the likelihood of the risk materialising and the potential impact of the risk on their business and reputation under different stress scenarios (see **Annex D** for more guidance).

6.3.10 Other relevant information for assessing likelihood and impact includes the past experience of similar institutions, and any changes in the external environment or within individual AIs (e.g. portfolio, organisational, personnel or system changes) which could have an effect on the assessment.

Risk control

6.3.11 AIs should consider the appropriate response actions to address the risks identified, taking into account the risk assessment results. For example, they can determine which of the risks –

- warrant active management attention, specific action and allocation of resources;
- may be best handled by contingency plans (see also section 7 for more details); or
- need periodic review to keep track of their status.

6.3.12 For those risks that require specific action (e.g. strengthening existing controls), action plans should be drawn up to facilitate subsequent monitoring of the progress made.

6.3.13 For those risks that may be very difficult or too costly to eliminate entirely (e.g. the threat of a terrorist attack), AIs may consider developing contingency plans as response actions. Normally, such a plan will not be invoked unless the event specified occurs. Where feasible, the plan can be coupled with insurance.[9]

6.3.14 For those risks that may be tolerated for the time being, AIs should keep them under periodic review to ensure that their status is unchanged and the approach of not taking any specific action remains appropriate.

[9] If insurance is sought, AIs should consider, among other things, the effect of any limiting conditions and exclusion clauses that may restrict cover to a small number of specific operational losses and may exclude larger or hard-to-quantify indirect losses (e.g. costs resulting from loss of business or damage to reputation).

6.3.15 All response plans (including contingency plans) should be approved by the Board, its delegated committee, or management at the appropriate level depending on their significance, and subject to periodic review to ensure that the progress is on track and the response actions implemented are effective. However, if a change in the risk profile suggests that the agreed actions should be modified, an ad hoc review should be promptly conducted and the relevant plans should be updated accordingly.

6.4 Risk monitoring and reporting

6.4.1 AIs should designate appropriate staff responsible for –

- ensuring that the response actions agreed for addressing specific risks are effective in keeping the risks under control;
- reviewing the response plans drawn up and identifying any need for modification;
- monitoring the proper implementation of the plans; and
- reporting the progress of implementing the plans and other relevant issues or developments to the appropriate level within an AI. For example, senior management should report to the Board or its delegated committee in respect of those risks deemed to be of top priority.

6.4.2 Apart from the regular monitoring and review of response plans, AIs should have in place effective early warning systems to help track the risks affecting reputation and provide red flags before a risk starts to develop into a direct threat to reputation. These systems will allow the Board and senior management to take prompt corrective actions to address any emerging threat, and be better prepared for any anticipated reputation event in advance. See subsection 6.5 for more details.

6.5 Early warning systems

General monitoring

6.5.1 A thorough monitoring system is a pre-requisite for obtaining early warning of potential risks to reputation. Such monitoring includes, for example, (i) monitoring of media reports covering AI-specific or business-specific issues and (ii) monitoring of

industry, market, political, legislative or social developments which may have implications for individual AIs. Much of this monitoring activity may already be a part of an AI's day-to-day operations. It is however important to note that any form of monitoring of relevant information sources will be of value to reputation risk management only if –

- the staff carrying out the monitoring activity are made fully aware of the reputation risk dimension and have a clear idea of what they are looking for; and
- there are channels to ensure that anyone spotting what might be early warning signs can get the information quickly and accurately into the right hands (e.g. those responsible for managing reputation risk).

Early warning indicators

6.5.2 Early warning systems may also involve developing and monitoring –

- performance indicators[10] and other indicators reflecting stakeholder confidence[11] which can provide a gauge of an AI's reputation and keep track of the progress in managing associated risks; and
- early warning indicators (e.g. a sudden increase in customer complaints, breaches of internal controls, operational errors, system outages, fraudulent incidents, and any significant deterioration in other performance indicators mentioned above) and any other triggers or thresholds which can act as alarm bells for management actions or provide signals to invoke any response or contingency plans.

6.5.3 The above-mentioned indicators should be reassessed and recalibrated periodically to ensure that they –

- are sufficiently effective and forward looking;
- are "fit for the purpose" in managing reputation risk; and

[10] These may include indicators in relation to business, management and staff performance, service standards, customer complaints, regulatory compliance, and compliance with internal policies and codes of conduct.

[11] These may include indicators based on customer / employee surveys, staff turnover trends, rating agency reports, benchmarking studies and media reports.

- will deliver the desired effect.

6.5.4 AIs should involve all relevant staff in the design of early warning indicators, and use available expertise and experience to improve existing indicators and devise new ones in case of need.

6.5.5 It is particularly important that AIs should set up formal channels and escalation procedures to higher levels for employees to raise concerns about potential threats to reputation that they observe in their course of work.

6.5.6 AIs should also be alert to any clearly identified risks which are, or have a high chance of, developing into reputation events. For example, if an AI is currently engaged in wage negotiations with its staff, any stand-off or acrimony in those negotiations may suggest a strong possibility of industrial action. These risks can then be prepared for and controlled in advance (see subsection 7.3 for more details).

6.5.7 In some cases, early warning signs may be spotted randomly (e.g. as a result of identifying something significant during a conversation by chance), but this requires a high level of awareness of reputation risk within an AI.

6.5.8 Whatever the source of early warning, AIs should ensure that the relevant information is adequately utilised and acted upon quickly.

6.6 Communications and disclosures

Communications with stakeholders

6.6.1 Communications with stakeholders can take many forms, including annual reports, prospectuses, website information, annual general meetings, press releases, press conferences and media interviews. Whatever the form of communication, AIs should communicate clearly what they have achieved or are doing, and back up their statements with hard evidence; otherwise reputation may be affected.

6.6.2 Stakeholders expect AIs to communicate with them in a clear, honest, transparent and timely manner. To meet their expectations, AIs should designate specific personnel to manage communications with stakeholders and other public relation matters, and to ensure that all relevant statutory or non-statutory disclosure and reporting obligations are fully complied with (see paras. 1.4.2 and 1.4.3).

6.6.3 Designated staff should have adequate knowledge, experience and training in managing media relations, making public announcements, dealing with public enquiries and providing useful input regarding reputation matters. They have primary responsibility for ensuring that communications –

- are clear, relevant, accurate and consistent;
- contain all material issues of interest to stakeholders; and
- fully meet stakeholder information requirements and, where necessary, are tailored to meet the needs of particular groups.

Disclosures to stakeholders

6.6.4 AIs should seek to enhance the quality, transparency and scope of disclosure to enable stakeholders to have a better understanding of AIs' business performance and future prospects. This can enhance AIs' credibility which, in turn, can boost reputation.

6.6.5 However, disclosing too much information may not always be desirable as some of it may be commercially sensitive, too detailed or technically complex. Disclosing insufficient or incomplete information, on the other hand, is undesirable because stakeholders may feel uncomfortable and confused. AIs should therefore seek to strike an appropriate balance when deciding what information and how much information should be disclosed. They should also consider carefully at what time and in what form such disclosures should be made, as late disclosure or disclosure in an inappropriate form may tarnish reputation.

6.6.6 Nowadays, in addition to financial information, stakeholders are interested to know more about how AIs conduct their business. Therefore, AIs should be able to demonstrate, with increasing levels of detail, how they run their business and how material risks facing them are managed. For instance, they may consider outlining their corporate governance arrangements and risk management framework in greater detail in their annual reports and, where appropriate, going beyond minimum disclosure requirements by disclosing areas where they have embraced best practices rather than minimum practices which will help to further enhance their reputation.

6.6.7 Stakeholders also want to be kept informed when new trends or issues that are of concern to them emerge. Reluctance to respond to their concerns may leave AIs open to criticism or accusations. Therefore, AIs should avoid putting themselves into a position where they seek to cover up bad news by withholding information. Where weaknesses are identified, they should be quick in disclosing plans or actions to rectify them.

6.6.8 As mentioned, honest, accurate and complete disclosures can enhance AIs' credibility and reputation. False, misleading or deceptive disclosures can seriously damage reputation and may lead to prosecution no matter whether they are made intentionally or inadvertently. Thus, AIs should ensure that all statements and information (including both financial and non-financial) provided by them are published or disclosed in an honest and accountable manner. Where necessary, senior management may consider conducting an independent review or audit to ascertain this.

6.7 Independent reviews and audits

6.7.1 The Board and senior management of an AI have ultimate responsibility for ensuring the integrity and effectiveness of its reputation risk management. They should therefore ensure that independent reviews and audits, whether as a review dedicated to reputation risk or as part of a wider review of risk management, are conducted regularly so as to provide them with assurance and confidence that controls and actions to manage the risks affecting reputation are operating as intended.

6.7.2 The main objective of independent reviews and audits is to ensure the robustness of the risk management process in identifying and managing risks affecting reputation, particularly to ensure that –

- no major threats to reputation remain unidentified;
- the responses to control or mitigate the identified risks are appropriate and implemented effectively;
- early warning systems developed to give advance warning of impending reputation problems are adequate and functioning well; and

- the reputation risk management process is effective and remains dynamic so that the changing status of the identified risks can be monitored and emerging threats to reputation can be picked up and acted on promptly.

6.7.3 Independent reviews and audits can be conducted by an AI's independent risk control function, internal auditors or compliance officers or by their combined effort. The manner in which these reviews and audits are to be performed (e.g. scope, frequency and by which party) may vary, depending on individual AIs' needs, their size and complexity, and the risks inherent in their business.

6.7.4 The results of such reviews and audits, including any issues and weaknesses identified, should be promptly and directly reported to the Board and senior management so that they can take early remedial actions, where necessary.

7. Management of reputation events

7.1 Overview

7.1.1 An AI may have taken all reasonable steps to anticipate and guard against potential threats to its reputation. However, if an event posing a direct threat to reputation happens and the AI is caught unprepared or responds inappropriately, its reputation may still be damaged. On the other hand, swift and positive responses to reputation events may even enhance an AI's reputation, and lower the risk of triggering a crisis. Therefore, in addition to maintaining an effective reputation risk management process, AIs should have in place an appropriate approach to managing reputation events.

7.1.2 Failure to properly manage a reputation event could, in some cases, also affect the reputation of an AI's directors and senior executives.

7.1.3 Reputation events differ in terms of the nature and level of severity. Although less serious events would not cause immediate concern, they should not be overlooked. Frequent occurrence of such events may lead to a perception that the AI concerned is "injury-prone".

7.1.4 A severe reputation event (e.g. fraud losses threatening an AI's survival) could be a crisis in its own right. It could also lead to other problems such as a liquidity crisis or emergency situations (e.g. disruption of normal business operations). In

all such cases, AIs should immediately invoke their crisis management procedures to handle the situations (see LM-1 "Liquidity Risk Management" and TM-G-2 "Business Continuity Planning" for more guidance).

7.1.5 This section focuses mainly on AIs' management of reputation events, which involves taking appropriate steps to contain or reduce the damage caused by those events and their after-effects, and to restore reputation where practicable. Subsections 7.2 and 7.3 provide some general principles and guidance to AIs on how to prepare for reputation events and structure action plans while subsection 7.4 highlights some considerations for protecting reputation in an event which has escalated into a crisis.

7.2 Approach to managing reputation events

General

7.2.1 The approach to managing reputation events and crisis situations can be quite similar in a number of aspects, except that crisis management usually involves the most senior executives of an AI (such as the Chairman of the Board and the Chief Executive), a larger number of supporting staff and more complicated procedures. Depending on the nature and severity of individual reputation events, the involvement of management and staff and the procedures applicable to such events vary. In some cases (e.g. those associated with management issues), the involvement of independent directors is desirable. Set out in **Annex E** is some general guidance on the key elements of crisis management which AIs may take into account in developing their approach to managing reputation events.

7.2.2 An AI's approach to managing reputation events, including any relevant strategy and policies, should be approved by the Board or its delegated committee and subject to periodic review and update by senior management to ensure that it remains appropriate over time. In addition, the approach should be well documented and communicated to all relevant personnel.

Overall strategy / action plan

7.2.3 As each reputation event is different, a precise list of actions which may be taken to deal with the event cannot be clearly specified. Nevertheless, AIs should take into consideration

some general guidance set down below in developing their overall strategy and action plan for handling reputation events:

- AIs' ability to communicate the right messages to the right people at the right time is crucial for limiting damage to their reputation. Judging from the experience of many past reputation events, timely report and escalation of a reputation event to senior management will be very helpful to the management of the event and the formulation of an action plan to deal with it. The effectiveness of the communication strategy and techniques should be the prime focus of any action plan to be undertaken.
- Controlling the situation is critical to successful management of reputation events. This is achieved by staying ahead of what has happened and anticipating developments before they happen.
- AIs should seek to gain time for planning action in advance through early recognition of warning signs and emerging threats (see subsection 7.3 for more details).
- While detailed actions will vary from case to case, a proper action plan covering some key areas should be formally structured. These include –
  - setting clear and precise objectives to be achieved;
  - defining the target audiences with whom AIs will be communicating and considering how their respective areas of interest or concern can be addressed;
  - deciding the key messages to get across to the target audiences. While the messages for different audiences may vary, they should not be contradictory or inconsistent;
  - establishing an overall strategy so that individual actions to be undertaken are coherent and mutually supporting;
  - ensuring that specific actions to be undertaken conform to the agreed strategy and objectives; and
  - controlling the timing of all proposed actions. Although the timetable may have to be adjusted as the action plan develops, it is important to maintain a time schedule of events from the start.

- AIs should consider how the facts of the situation can be presented to target audiences in a manner which will win their acceptance and understanding. However, in no case should false information or distorted perspectives be presented.
- In limiting damage to an AI's reputation, emphasis should be placed on demonstrating to target audiences –
  - how much care the AI has taken to guard against the recurrence of similar events; and
  - the actions taken by the AI in response to the event and the effectiveness of its actions.
- To ensure that consistent messages are disseminated, the same person (or team of persons) should be designated to handle all communication matters, including media relations and public announcements.
- Actions taken should be based on a thorough knowledge of the facts of the situation, and be planned with a clear understanding of the likely consequences (including any follow-up action which may then be required).
- In the case of AIs with cross-border operations, actions taken should cater for any possible impact on those operations.
- AIs should ensure that the management structure for dealing with reputation events facilitates speedy and effective implementation of agreed actions.
- All relevant parties within an AI should be adequately briefed as the situation develops.

7.2.4 As the points mentioned above are not exhaustive, AIs should tailor their strategy and action plan to suit their specific circumstances and needs.

Process

7.2.5 Reputation events may come suddenly, and almost certainly, carry with them some unexpected elements. It is therefore important for AIs to establish a clear set of procedures for managing such events (including pre-planning how certain situations may be handled). These include –

- defining reputation events to be captured (e.g. through pre-determined criteria, triggering conditions or

hypothetical scenarios, etc.). In determining what types of events to be included, AIs should have regard to the results of their internal processes for identifying and assessing reputation risk, as well as their vulnerability to reputation risk;

- specifying the process for identifying reputation events, including the authority[12] for deciding whether a reputation event has occurred and for invoking procedures for managing the event;
- assessing the impact of such events based on established standards and criteria (with particular focus on the impact on the AI's business and reputation);
- establishing appropriate response actions [13] (see also para. 7.2.3), such as how to deal with the event in question and to protect the AI's reputation (e.g. issuing a press release to address public concern), and prioritising agreed actions according to the AI's needs;
- notifying all parties concerned (such as home / host supervisors, relevant business partners and counterparties) promptly about the situation they are faced with;
- implementing agreed actions and monitoring subsequent developments (particularly public reaction to actions taken);
- reassessing the situation and, in case of need, modifying agreed actions;
- ongoing reporting to the Board and senior management of the progress and results of implementing agreed actions; and
- enhancing reputation risk management, where necessary, after the event has been settled, based on experiences gained and lessons learnt.

Roles and responsibilities

[12] Such authority should normally be restricted to staff at the management level (e.g. department head level).

[13] These may be in the form of action checklists summarising key decisions and tasks which should not be missed when dealing with a reputation event.

7.2.6 AIs should designate appropriate personnel to be responsible for formulating, implementing and coordinating the approach to managing a reputation event when it happens. A focused team may also need to be formed to deal with the specifics of individual events. Membership of this team will probably differ from case to case, as the circumstances of each event vary. For example, an IT-driven reputation event will need to involve the IT manager on the team.

7.2.7 AIs should ensure that there is a clear definition of roles and responsibilities so that all persons involved in managing a reputation event are fully aware of their responsibilities and understand what is expected of them at the time of dealing with the event (e.g. the required procedures under their responsibilities).

Post-event reviews

7.2.8 After an AI has experienced a reputation event, the Board and senior management should consider the need for conducting a post-event review to identify any lessons learnt, or problems and weaknesses revealed, from the event. Such reviews will be useful for providing feedback and recommendations for enhancing the AI's reputation risk management process, and should at least be conducted on any major event affecting the AI.

7.2.9 The Board and senior management should be promptly informed of the results of any such review conducted so that they can take appropriate actions to improve the AI's approach to managing reputation risk.

7.3 Preparation and early action

7.3.1 AIs' implementation of early warning systems (see subsection 6.5) will enable them to plan actions in advance for addressing potential threats that are likely to develop into reputation events. Early recognition of impending reputation problems also means that valuable time has been won to facilitate pre-planning for future action.

7.3.2 For perceived risks identified to have developed, or have a high chance of developing, into direct threats to reputation, AIs should consider the necessary steps to be taken, including –

- reassessing the latest situation and making decisions about what actions could be taken to resolve the problem and how such actions should be implemented;
- checking if all information on the situation has been assembled and taken into account;
- reviewing any existing plans (e.g. contingency plans) for dealing with a risk of this nature, and modifying them as necessary to reflect actual circumstances;
- informing all relevant personnel (including those directly involved in implementing planned actions) to ensure that they are kept fully appraised of the situation;
- ensuring that all necessary support and communication systems are in place;
- putting together an action plan that can be readily implemented in case of need; and
- reporting the issue and the action plan to the Board and, where appropriate, the HKMA.

7.4 Managing reputation in a crisis

7.4.1 In the case of a full-blown crisis which has emerged from a reputation event, concern over an AI's reputation will be secondary to other more important priorities, such as –

- preventing any threat to the AI's survival;
- ensuring minimum disruption to the AI's normal business operations and services;
- minimising any distress or concern to individuals or groups affected by the crisis (e.g. depositors during a bank run); and
- protecting the AI's commercial interests.

7.4.2 Nevertheless, effective implementation of the above-mentioned priorities will help protect the AI's reputation and reduce long term damage to the business. Adopting good communication strategies during a crisis will also serve the dual role of managing the crisis and protecting the AI's reputation.

Annex A : Reputation risk profile - summary of major characteristics[14] by risk category

Risk category		
Low	**Moderate**	**High**
• No negative publicity regarding the AI's business practices is noted, and franchise value is only minimally exposed by reputation risk. • The AI has a good track record on regulatory compliance, and does not regularly experience litigation or customer complaints. • Losses from fiduciary activities are low relative to the number of accounts, the volume of assets under management and the number of affected transactions. • Exposure from reputation risk is expected to remain low in the foreseeable future. • Management anticipates and responds well to changes of a market or regulatory nature that impact the AI's reputation in the marketplace. • Management fosters a sound corporate culture that is well supported throughout the organisation, and has proven very effective over time. • The AI is well-versed in managing complex risks and effectively self-polices risks. • Reputation risk management is strong, with effective procedures to protect the AI from potential threats to reputation and to mitigate the effects of reputation events should they occur. • Internal controls and audits are fully effective.	• Negative publicity regarding the AI's business practices is not serious, and the exposure of franchise value from reputation risk is controlled. • No significant cases of regulatory non-compliance, both in terms of number and nature, are noted. • The level of litigation, losses, and customer complaints are manageable and commensurate with the volume of business conducted. • Exposure from reputation risk is not expected to increase in the foreseeable future. • Management adequately responds to changes of a market or regulatory nature that impact the AI's reputation in the marketplace. • The AI has avoided conflicts of interest and other legal or control breaches. • The AI effectively self-polices risks, and has a good record of correcting problems. • Reputation risk management is generally satisfactory, and there are established procedures for controlling reputation risk and handling reputation events. • Internal controls and audits are generally effective.	• Negative publicity regarding the AI's business practices is increasing, and franchise value is substantially exposed by reputation risk as shown by significant litigation, substantial dollar losses, or a high volume of customer complaints. • Regulatory compliance is unsatisfactory, and no significant improvement in this area is noted. • The potential exposure from reputation risk is increased by the number of accounts, the volume of assets under management, sales practices of complex products, or the number of affected transactions. • Exposure from reputation risk is expected to increase in the foreseeable future. • Management does not anticipate or take timely or appropriate actions in response to changes of a market or regulatory nature. • Poor administration, conflicts of interest and other legal or control breaches may be evident. • The AI's performance in self-policing risks is suspect. • Weaknesses may be observed in one or more of the critical operational, administrative, or investment activities. • Management information at various levels of the AI exhibits significant weaknesses. • Reputation risk management is unsatisfactory, without proper systems for controlling reputation risk and handling reputation events. • Internal controls and audits are less than effective in reducing exposure. • Management has either not initiated, or has a poor record of, corrective action to address problems.

[14] This Annex is compiled for AIs' reference only. The characteristics shown are not necessarily all-inclusive, and every characteristic within a risk category does not have to be met in order for an AI to be categorised under that risk category.

Annex B : Key drivers of reputation

B1 Introduction

B1.1 This Annex provides AIs with more information about the key drivers of reputation mentioned in subsection 3.2. In particular, it analyses how each of these drivers may affect reputation risk and highlights some considerations for managing their effects on reputation.

B2 Corporate governance

B2.1 Good corporate governance is vital to an AI's reputation. This is because the leadership of the Board and senior management and their capability to run the business and manage risks will directly affect stakeholders' perception of the AI. Reputation can be impaired if, for example, the AI lacks a clear vision for the future, its leadership is seen to be poor and incompetent, or a number of governance issues have hampered effective functioning of the AI.

B3 Management integrity

B3.1 Management integrity has been the cause of some bank scandals in the past. As the personal ethics and behaviour of an AI's directors and senior management (e.g. the Chief Executive and key managers) are important determinants of stakeholder confidence, the probity and conduct of such persons will always be under close scrutiny by its stakeholders.

B4 Staff competence / support

B4.1 Staff competence and support is essential for business success. Given that human capital is an important asset, AIs' ability to harness it to meet their business objectives will enhance reputation. This will depend, for example, on whether they can –

- recruit, develop and retain high quality staff; and
- motivate staff and satisfy their needs (e.g. by providing appropriate remuneration and incentive schemes, a healthy and safe working environment, etc.).

B4.2 Deficiencies in employment and staff management practices, however, could lead to various problems, including high staff turnover, insufficient staffing, poor service quality, staff incompetence / misconduct, customer complaints and employee disputes. Some of

these problems may result in damaging headlines and adverse publicity.

B5 Corporate culture

B5.1 If an AI's corporate culture is seen to inadequately support the achievement of its business objectives and effective risk management, it may arouse stakeholder concerns and result in a loss of confidence.

B5.2 It is therefore crucial for AIs to promote a corporate culture where –

- the adoption of ethical and responsible behaviour that can protect and enhance their reputation is encouraged;
- compliance issues or lax control standards are not tolerated; and
- there is an established mechanism for employees to voice concerns if they are aware of any potential threats to reputation (e.g. business malpractices, suspicion of fraud, etc.).

B6 Risk management and control environment

B6.1 A sound risk management and control environment is essential for AIs to safeguard their assets and capital, and to mitigate reputation risk. Although there is no guarantee that the institution of adequate risk management and controls will always prevent fraud and abuse, such acts will be able to be perpetrated more easily if the overall risk management and control environment is weak. AIs should seek independent assurance that existing risk management and control systems are running properly (e.g. through internal audits) and be vigilant for, and take necessary actions to counter, any deterioration in risk management and control standards.

B7 Financial soundness / business viability

B7.1 An AI's reputation is likely to suffer if its financial soundness or business viability is called into question. For example, substantial losses resulting from an AI's unsuccessful investments or business operations may spark immediate concerns from stakeholders (in particular, shareholders, investors, or analysts) about whether the AI is still a safe investment or of long term business value. Such concerns may spread quickly to other aspects of reputation (e.g. management competence) as well.

B7.2 To safeguard and bolster reputation, AIs should build up stakeholders' trust in their financial reporting systems (e.g. that their financial

exposures are fairly represented), and be able to manage stakeholders' expectations by providing relevant factual information to facilitate their assessment of AIs' financial performance (e.g. explaining any problems promptly, with timely actions to rectify them) and future prospects (e.g. outlining future business plans and sources of growth).

B8 Business practices

B8.1 AIs are required to run their businesses in a responsible, honest and prudent manner. Business practices which deviate from this basic standard could erode stakeholder confidence and irreparably damage their reputation, and any resultant breach of laws and regulations (e.g. adopting improper selling practices, engaging in unauthorized activities, etc.) may lead to investigations, disciplinary actions and criminal charges. In dealing with customers and other counterparties, AIs should be guided by, and closely adhere to, all relevant ethical standards and codes of conduct.

B8.2 AIs' reputation will also be influenced by their willingness and ability to honour their own obligations and commitments, whether contractual or otherwise. In this regard, AIs should be particularly alert to situations in which they might have entered into arrangements that carry reputation risk (e.g. by taking on moral obligations to support those arrangements in case of need). A typical example of such arrangements is bank-sponsored structured investment vehicles ("SIVs") in which the sponsoring bank may feel compelled on reputation grounds to come to the rescue of a troubled SIV.

B8.3 Increasingly, AIs should be aware of the possible impact on their reputation of other social and environmental responsibilities expected of them by such stakeholders as customers and pressure groups. For example, AIs may be expected to implement environmentally friendly policies (e.g. green policies or energy saving programmes) and provide for customers with special needs (e.g. handicapped or visually impaired customers).

B9 Customer satisfaction

B9.1 AIs' ability to satisfy customer needs and expectations on a continuing basis is of paramount importance in sustaining their business in a highly competitive banking environment. Failure to do so, as illustrated by the following examples, may result in loss of customer

confidence, falling business, adverse publicity or, in some cases, legal sanctions:

- Unfair treatment of customers – customers may have been over-charged or inaccurately billed, or have suffered losses due to an AI's errors or omissions (e.g. customer instructions not properly executed) without obtaining fair compensation;
- Mis-handling of customer information – customers' confidential information may have been inadvertently destroyed, lost or exposed to third parties, thereby breaching AIs' confidentiality obligations and privacy rules relating to personal data;
- Unreliable / inefficient banking services – frequent system outages, significant operational errors and oversights, and inefficient processing systems will weaken customer confidence in an AI's capacity to deliver quality services. Lack of new / innovative products and services to suit changing customer needs may also arouse discontent;
- Mis-handling of customer complaints – customers expect AIs to be responsive to their concerns. A poor complaint-handling system runs the risk of damaging customer goodwill and overlooking early indicators of potential threats to reputation; and
- Business malpractices – customer confidence will be greatly impaired if AIs are found to have engaged in improper or illegal business practices (as mentioned above).

B10 Legal / regulatory compliance

B10.1 Breaking the law or contravening any relevant regulatory standards and guidelines (either deliberately or inadvertently) can lead to serious consequences, including regulatory investigations, costly and high profile litigation, public censure, civil and criminal sanctions, harmful publicity, claims for damages, or even the loss of authorization. There may be significant damage to an AI's reputation even if the AI is ultimately acquitted of any illegal conduct.

B10.2 AIs should therefore adequately appraise legal and regulatory risks, and put in place robust systems to ensure compliance, including enhancing staff awareness of compliance issues and identifying areas of potential threat and vulnerability.

B11 Contagion risk / rumours

B11.1 AIs operating as part of a group (comprising banking or non-banking entities) will be susceptible to reputation events affecting their parent bank, non-bank holding company, or other members of the group (e.g. sister companies, subsidiaries and affiliates). For example, an AI's reputation may be damaged by regulatory sanctions against its parent bank for, say, breach of anti-money laundering regulations or by publicised concerns about the parent bank's safety and soundness (e.g. due to substantial trading losses).

B11.2 Such contagion effects on AIs' reputation may also result from other problematic relationships, such as any close association (whether knowingly or unknowingly) with major customers, counterparties or service providers that are revealed to be engaged in unethical, unlawful or corrupt activities.

B11.3 Rumours, even though unfounded, about an AI (or parties closely associated with the AI) may have a damaging impact on the AI's reputation and the level of public confidence in the AI if no quick, decisive actions are taken to quell the rumours. Therefore, AIs should always be on the alert to the spreading of rumours and the effects of rumours, which could be exacerbated by such factors as the general weakening of public sentiment due to unfavourable or worsening market conditions or the instigation of adverse news reports on particular AIs. It should also be noted that rumours about an AI may spread more easily if market perception is that the AI is weak.

B11.4 Adequate contingency procedures should be developed to deal with the above situations.

B12 Crisis management

B12.1 An AI's inadequate response to a crisis, or even a minor incident, that attracts media attention could arouse stakeholder concerns about management competence, thereby jeopardising the AI's reputation. On the other hand, effective crisis management arrangements (including communications with stakeholders and the media) could quickly allay stakeholder fears, restore their confidence and even enhance reputation.

B12.2 AIs should therefore ensure that they are ready to deal with possible crises (which may be unprecedented and totally unexpected), with detailed and well-rehearsed crisis management plans in place. Close attention should also be paid to managing media communications

(e.g. making sure AIs are accessible and available for comment during a crisis).

B13 Transparency / accountability

B13.1 AIs' ability to be responsive to and satisfy stakeholders' information needs (e.g. by disclosing information in respect of material issues of interest to stakeholders in a transparent, honest and prompt manner) has itself become a key determinant of business competence. Such information will help stakeholders in understanding AIs' values, strategies, performance and future prospects.

B13.2 Stakeholder confidence, as well as AIs' credibility and reputation, will however be weakened if information disclosed is found to be misleading, inaccurate or incomplete. As such, there should be adequate accountability for the integrity of information disclosures, which should be backed by robust management monitoring and reporting systems.

Annex C : Use of risk register for identification, assessment and control of reputation risk

C1 Introduction

C1.1 This Annex illustrates how Bank A (a hypothetical AI) makes use of a risk register to document the processes for identifying, assessing and controlling the risks affecting its reputation. AIs should regard this illustration as for reference only. They should devise an approach that suits their own circumstances and needs.

C2 Background

C2.1 As part of the reputation risk management process, Bank A develops a risk register that enables a comprehensive review of the status and significance of the risks affecting its reputation as well as the approach adopted to address the risks identified.

C2.2 Risk Control Department ("RCD") of Bank A maintains the risk register for the bank as a whole. Among other things, RCD is responsible for –

- ensuring that the details recorded in the risk register are relevant and up-to-date, and
- all decisions arising from the reputation risk management process have been properly approved before they are entered into the risk register.

To perform these duties, RCD is required to liaise closely with other relevant departments and to monitor their performance in accordance with their assigned roles under the reputation risk management process.

C3 Risk identification

C3.1 Bank A defines the sources of reputation risk as those events or situations that could hinder the achievement of its strategic goals and objectives, the satisfaction of the needs and expectations of its major stakeholder groups, and hence the maintenance of a good reputation. This definition, which is approved by the Board and documented in the risk management policy, forms the basis for identifying the risks affecting the bank's reputation.

C3.2 Bank A requires all major departments to complete questionnaires on reputation risk and reflect their views on what they consider as the key

sources of reputation risk affecting their own department and the bank as a whole. Such questionnaires solicit other related information on what has caused the risk, how the risk is being managed, and the level of significance of the risk (see sections C4 to C6). RCD collates the results and arranges follow-up workshops or discussions with the participating staff where necessary. Other relevant sources of information, such as media reports, customer satisfaction surveys and performance indicators, are also taken into account for risk identification purposes.

C3.3 Bank A uses the risk register to record the risks identified from the process, which are broadly classified into the following categories:

- Operating environment (e.g. issues arising from market, political, social, regulatory and technological developments);
- Stakeholder relations and communications (e.g. issues relating to stakeholder loyalty and confidence, satisfaction of their needs and expectations, and effective communications with them);
- Strategic planning and business development (e.g. issues relating to setting and fulfilment of goals and targets, business performance and profitability, market standing and competitive situation, and business outlook);
- Human resources (e.g. issues relating to recruitment, retention, and succession planning, remuneration and incentive schemes, competence and training, motivation, conduct and integrity, morale, staffing and workload, health and safety, etc.);
- Systems, controls and infrastructure (e.g. issues relating to information, data and security management, operations and processing, supporting systems and infrastructure, risk management processes and controls, financial and budgetary controls, business continuity and crisis management);
- Legal and regulatory compliance (e.g. issues relating to compliance with relevant laws, regulations and codes of conduct, impact on authorization / licensing status, etc.);
- Corporate governance (e.g. issues relating to governance infrastructure and practices, and compliance with internal policies, codes of conduct, guidelines and procedures); and
- Other reputation issues not covered above (e.g. issues arising from contagion risk, pressure group interest and media relations).

C3.4 Each identified risk recorded in the risk register is required to have a clear risk description that reflects the nature of the risk as well as the

potential effects on reputation. For example, one of the risks identified under the category of "systems, controls and infrastructure" relates to "poor custodial controls over customer assets". The risk is described as "poor custodial controls over customer assets resulting in an increased risk of fraud and litigation which may in turn lead to adverse publicity and damage to reputation".

C4 Risk assessment

C4.1 To determine whether the risks identified are significant and worthy of attention, Bank A prioritises the risks by "likelihood" and "impact" using a simple three-by-three matrix (i.e. ranking each risk by "high", "medium" or "low" for both the "likelihood" and "impact" ratings).

C4.2 As an illustration of how the matrix works, if the risk identified is customer dissatisfaction with Bank A's service quality leading to account closures, the "likelihood" and "impact" ratings will depend on Bank A's assessment of the probability of the risk materialising and the estimated drop in customer accounts as a result. Assuming Bank A gathers from various performance indicators that the likelihood of customer dissatisfaction (characterised by failure to meet its servicing standards) is high (say, with more than a 70% chance) and the total number of customer accounts is likely to drop significantly by over 10% within a month based on past surveys or statistics, both the "likelihood" and "impact" ratings may be classified as high. If, instead, the likelihood of customer dissatisfaction is low (e.g. below a 10% chance) due to stringent enforcement of customer service quality, the "likelihood" rating will be low but the "impact" rating will remain as high.

C4.3 Where appropriate, Bank A also performs other analyses such as control assessment and stress-testing (see para. 6.3.9 for more details) to assess the "likelihood" and "impact" ratings.

C4.4 Bank A requires that the risk assessment incorporates the views and feedback of all relevant parties, including those departments or units to which the risks relate.

C5 Risk control

C5.1 Based on the risk assessment results, Bank A formulates the response plans by considering which of the following options should be adopted for each of the risks identified:

- Transfer option – this means sharing the risk in whole or in part with another party (e.g. by outsourcing the activity) or by insuring

all or part of the risk. Bank A however understands that its reputation could still be affected if things go wrong;

- Terminate option – this involves taking steps to withdraw from the activity causing the risk or to avoid situations that could trigger it;
- Treat option – this means bearing the risk but reducing its likelihood (e.g. through strengthening controls) and/or impact (e.g. through contingency planning) to keep the risk within an acceptable level; and
- Tolerate option – this means taking no additional actions for the time being but keeping the risk under review from time to time.

C5.2 Bank A requires that –

- where a risk is treated, specific action plans should be developed with timelines and measurable objectives to facilitate subsequent monitoring. For those risks that are difficult to control, contingency plans should be drawn up; and
- where a risk is tolerated, a periodic review of the risk should be conducted to ensure that the "tolerate" option remains appropriate.

C5.3 For controlling purposes, Bank A designates a risk owner for each of the risks identified. The designated risk owner assumes overall responsibility for ensuring that any actions agreed for dealing with the risk concerned are properly carried out and have the desired effect (see para. 6.4.1 for more details).

C5.4 Bank A requires that all response plans (including contingency plans) be duly approved and subject to periodic review.

C6 Risk documentation

C6.1 Bank A records all pertinent details evidencing results of the risk identification, assessment and control processes in the risk register. For each identified risk, these details include –

- risk description;
- root causes of the risk (or the core issue(s) involved);
- existing controls to manage the risk (and their effectiveness);
- risk assessment (likelihood and impact);
- designated risk owner; and

- response plan and agreed actions.

C6.2 The risk register is regularly reviewed and promptly updated to reflect changing circumstances and developments.

Annex D : Supplementary guidance on use of stress-testing for reputation risk management

D1 Introduction

D1.1 As illustrated from the market turmoil that began in mid-2007, reputation risk is one of the risk factors that could potentially affect the business and financial performance of banks. It also has close links with other major risks, such as credit, market and liquidity risks. This Annex sets out some guidance on how AIs may take account of reputation risk in their stress-testing procedures.

D1.2 This Annex should be read in conjunction with IC-5 "Stress-testing", which provides general guidance on the use of stress tests for risk management purposes.

D2 Stress-testing for reputation risk

D2.1 As required under IC-5, AIs should adopt an integrated approach to stress-testing and produce stress-testing results on an institution-wide basis, covering stress events that cater for the major types of risk they are faced with. As such, AIs employing stress-testing techniques for assessing reputation risk should seek to incorporate stress scenarios for reputation risk into their institution-wide stress-testing procedures and assess the impact of reputation risk on other major risks (e.g. credit or liquidity risk).

D2.2 In developing stress scenarios for reputation risk, AIs should identify major sources of reputation risk to which they are potentially exposed or an appropriate range of circumstances and events in which reputation risk would crystallise (see **Annex B** for more details about key drivers of reputation). AIs should also consider how those sources, circumstances and events may adversely affect their business prospects and financial position (including earnings, capital and liquidity) as well as generate other second-round effects[15].

D2.3 The recent market turmoil provides insight into some examples of potential reputation risk which AIs may take into account when formulating their stress scenarios and parameters. These are highlighted below for AIs' reference.

---

[15] This term refers to the effects that the initial impact of a shock (e.g. rumours or scandal) on an AI has on its balance sheet (e.g. loss of customer deposits, closure of accounts, etc.) and the rest of the banking system (e.g. contagion effects on other AIs of similar size and profile).

- In stressed conditions, some banks may go beyond their contractual obligations to provide credit or liquidity support to their sponsored securitization structures and off-balance sheet vehicles (such as ABCP conduits and SIVs) on reputation grounds. Some other banks may purchase ABCP issued by their sponsored vehicles in order to maintain market liquidity. As a result, these banks will assume additional liquidity, market and credit risks and also put pressure on their capital ratios (especially when this involves a bank putting back the assets it has securitized onto its balance sheet).
- Reputation risk may arise from a bank's involvement in asset management, investment advisory or securities dealing activities, particularly when financial instruments, whether issued by entities owned or sponsored by the bank or by other parties, are distributed or sold to the bank's customers. In the event that the financial instruments were not correctly priced or the main risk drivers underlying the instruments were not clearly or adequately disclosed, the bank may be sued by its customers or face pressure to cover losses suffered by them.
- Similarly, reputation risk may arise when a bank sponsors activities such as money market mutual funds, in-house hedge funds and real estate investment trusts ("REITs"). In these cases, the bank may decide to support the value of shares / units held by investors on reputation grounds even though it is not contractually required to provide the support.
- Reputation risk may also affect a bank's decision to call its liabilities (including preferred shares or hybrid / subordinated debt that constitute regulatory capital). For instance, amid market concerns about its funding capacity, the bank may decide to maintain market confidence by exercising a call option to redeem a previous issue of subordinated debt, even though prevailing market conditions are unfavourable and such action may adversely affect the bank's liquidity profile and capital position.

D2.4 The above examples are not exhaustive. AIs may face reputation risk in other aspects, such as those arising from material weaknesses in their internal risk management processes (e.g. resulting in substantial fraudulent losses) or management's failure to respond swiftly and effectively to external threats or influences (e.g. resulting in poor strategic decisions). AIs should exercise their best judgement and apply stress scenarios and parameters that suit their own circumstances and risk profile.

D2.5 Once the potential exposures arising from reputation concerns are identified, AIs should estimate the amount of support (capital or liquidity) they may have to provide or losses they may experience under adverse market conditions. AIs should also assess the impact of reputation risk on other risks to which they may be exposed. This could be accomplished by including reputation risk scenarios in regular stress tests. For instance, non-contractual off-balance sheet exposures could be included in the stress tests to determine the effect on an AI's credit, market and liquidity risk profiles.

D2.6 In addition, AIs should assess whether there is any longer term impact on their business and operations due to reputation risk (e.g. loss of market share, customer base or business revenue). AIs should also pay particular attention to the effects of reputation risk on their overall liquidity position, taking into account both possible changes in the asset side of the balance sheet and possible restrictions on funding, should the damage in reputation result in a general loss of confidence on the part of their counterparties and customers.

D2.7 Senior management should actively participate in the conduct of stress-testing and scenario analyses for reputation risk (including the development of stress scenarios and assumptions), and thoroughly review and discuss the stress-testing outcomes. Where appropriate, the implications for an AI's strategy and business activities, and the need for taking mitigating actions (e.g. whether particular activities involving significant reputation risk should be curtailed), should be considered.

Annex E : Key elements of crisis management

E1 Introduction

E1.1 The main purpose of this Annex is to provide general guidance to AIs on the key elements of effective crisis management, which may apply to different types of crisis situations. AIs may take into account relevant guidance set out in this annex and other modules of the Supervisory Policy Manual (e.g. TM-G-2 "Business Continuity Planning"), and consider how the recommended practices could be incorporated into or merged with their existing business continuity and contingency planning arrangements.

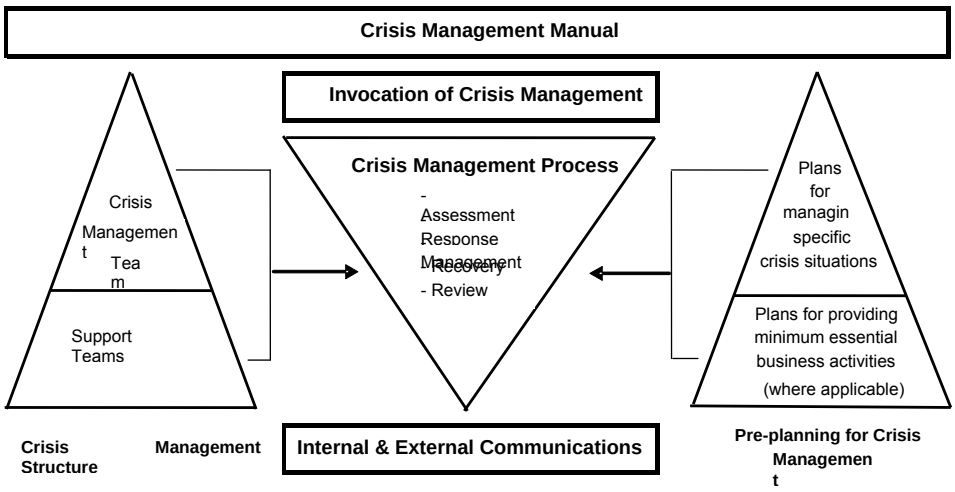
E2 Key elements of crisis management

E2.1 The key elements of effective crisis management include:

- crisis management manual;
- crisis management structure;
- invocation of crisis management;
- crisis management process;
- internal and external communications; and
- pre-planning for crisis management.

E2.2 **Diagram 2** below shows how the key elements mentioned above interact with each other.

Diagram 2 – Key elements of crisis management



E3 Crisis management manual

E3.1 A crisis management manual will provide an authoritative and readily available source of reference to AIs' management and staff for dealing with crises. The manual generally covers the following aspects:

- Approach – this outlines an AI's approach to managing situations that may threaten its business, operations and reputation, and includes relevant information such as crisis management strategies, rules and guidelines for response actions, processes, procedures and designation of responsibilities for all relevant personnel involved in the crisis management process (see sections B4 to B7);
- Scope – this defines the types of crisis situations to be dealt with in the manual. Such events may be described in terms of pre-determined criteria, triggering conditions, or hypothetical scenarios. To facilitate crisis management, there should be a system to analyse their level of severity;
- Crisis management plans – these plans are the result of pre-planning how different crisis situations are to be handled. They include plans for managing specific events and, where some level of business disruption has been caused, plans for providing minimum essential business activities (see section B8);
- Preparation / action checklists – such checklists serve the purpose of reminding all responsible personnel of the list of tasks that cannot be missed (e.g. establish clear lines of communication with certain key parties) and ensure that all required equipment and systems are in place during the crisis management process;
- Contact lists – all relevant internal and external contact lists should be maintained and kept up-to-date. The internal contact lists should provide key contacts of personnel within an AI, and alternate contacts in case the primary contacts are not available. The external contact lists should provide contact points of external parties with whom dialogue should be maintained in a crisis situation (e.g. regulators, key business counterparties, the media, the police, or other public services, etc.); and
- Draft "line to take" / press statements – these draft statements (or key messages to be disseminated) prepared in relation to some specified situations provide a ready source of reference. They are however subject to modification when an AI responds to the

actual situation, in the light of experiences and changing circumstances.

E3.2 AIs should decide on the degree of detail to be included in the manual to allow quick and easy reference. They need to strike a balance between (i) making the manual indigestible and difficult to absorb by including too many details and (ii) making it so general as to be of little value.

E4 Crisis management structure

General

E4.1 A crisis management structure that defines responsibility clearly would help minimise confusion and uncertainty when dealing with crisis situations. As there is no standard crisis management structure, the appropriate structure to be established depends on AIs' individual circumstances and needs. Generally, a crisis management structure may comprise a Crisis Management Team (i.e. CMT) and various support teams.

Crisis management team

E4.2 The CMT assumes overall responsibility for how an AI emerges from a crisis. Predominantly, it has a role in protecting the AI's business and reputation. In managing a crisis, the CMT should not confine itself to general decisions but should concentrate on key issues, direct the actions which the AI needs to respond to and, ultimately, control the situation. The CMT should also take responsibility for executive actions even though implementation of such actions will normally be delegated. Some specific responsibilities include –

- deciding upon strategies and response actions in relation to the crisis;
- identifying, where necessary, which business activities should be resumed or initiated as a matter of priority;
- managing the invocation of support teams; and
- monitoring and re-prioritising the needs of the AI until the crisis is over (i.e. the normal situation is resumed).

Support teams

E4.3 Support teams are broadly divided into two types:

- those that are responsible for dealing with the immediate crisis and handling external communications in accordance with the decisions and instructions of the CMT; and
- those that are responsible for providing support (such as carrying out administrative functions or technology recovery) to facilitate the implementation of the above-mentioned decisions and instructions.

Which persons should join the support teams entirely depends on whether there is a direct need for their expertise, knowledge and experience during the crisis management process. The size and number of support teams necessary for dealing with a crisis will also depend on the severity of the situation.

E4.4 Responsibilities of each support team and each of the team members (if they carry out different tasks) need to be clearly allocated and defined. Usually, the team leader is responsible for setting the team's priorities, tasking the team members and managing the current situation, while individual team members are responsible for completing tasks assigned to them quickly, efficiently and with minimum supervision.

E5 Invocation of crisis management

E5.1 AIs should establish a clear set of procedures for invoking crisis management procedures, including the authority for determining whether a crisis has occurred, and the corresponding procedures that should be invoked[16]. These procedures should be documented in their crisis management manual.

E5.2 From time to time, AIs may come across situations requiring judgement as to whether some of those situations would amount to a crisis and whether to report the case to senior management. AIs should, in particular, have a system in place for reporting, reviewing and deciding upon those situations. For example, appropriate personnel should be designated with the responsibility of (i) reviewing the situations reported by individual departments, functions or units, (ii) analysing their potential implications for an AI's business and reputation, (iii) monitoring their developments (if the issues are still unfolding), and (iv) proposing whether further actions need to be taken. Any significant matter would need to be urgently dealt with,

[16] Such authority should normally be restricted to senior personnel, for example, the Chief Executive, or the Chairman of the CMT. In the case of formally putting an AI into a crisis mode, members of the Board will also need to be immediately consulted or advised.

with immediate escalation of the case to the relevant decision-making parties, according to the procedures laid down in the crisis management manual. In case of doubt, it is advisable to err on the side of caution and report the case to senior management in order not to lose any time in dealing with what might turn out to be a major crisis.

E6 Crisis management process

E6.1 A sound crisis management process has the following phases:

Phase 1 - Assessment

- The activities under this phase generally include (i) initial impact assessment, (ii) establishing the appropriate response actions, such as how to deal with the crisis in question (e.g. issuing a press release to address public concern and safeguard public confidence), (iii) prioritisation of the AI's needs, and (iv) notifying all parties concerned (e.g. regulators and relevant business partners).
- As most of these activities require decision-making, the CMT will be deeply involved, with all support teams standing by to offer assistance. To facilitate decision-making, the CMT can make reference to the pre-considered plans prepared for crisis management.

Phase 2 – Response

- The activities under this phase generally include (i) assembling the support teams required to manage the crisis, (ii) setting up a crisis management centre with all necessary equipment and facilities in case of need, (iii) collecting updated information for the CMT to reassess the situation, and (iv) where necessary, modifying the agreed actions and/or priorities.
- Both the CMT and the support teams will be involved in the above activities, with the CMT making decisions (e.g. whether to set up a crisis command centre or modify agreed actions), and the support teams providing support to the CMT where applicable (e.g. collecting updated information, setting up necessary facilities and equipment, etc.).

Phase 3 – Management

- The activities under this phase generally include (i) implementation of the agreed actions, (ii) maintenance of a

continuous log of events, (iii) closely monitoring developments of the crisis (particularly public reactions to the crisis), (iv) ongoing reporting of the progress of implementation and monitoring to the CMT to facilitate their reassessment of the situation, and (v) where necessary, modification of agreed actions and/or priorities.

- Under this phase, all relevant support teams need to actively participate in the actions required to manage the crisis, and the CMT is mainly involved in making decisions and overseeing the overall crisis management process until the crisis is over.

Phase 4 – Recovery (where applicable)

- The activities under this phase generally include (i) establishing an approach to business recovery (i.e. resumption of an AI's normal day-to-day operations), (ii) planning for implementation of the approach, and (iii) executing the implementation plan.
- Under this phase, the involvement of the CMT is minimal as the responsibility for recovering the business in full is usually undertaken by the AI's management with assistance from various departments and, where necessary, the support teams.

Phase 5 – Review

- The activities under this phase generally include (i) highlighting the problems revealed from the crisis, (ii) learning lessons from the problems, and (iii) where appropriate, providing feedback for enhancing the crisis management process based on experiences gained from the crisis.
- As this phase will usually be undertaken when a crisis is over, the AI's senior management usually takes charge of the activities and is responsible for reporting the review results to the Board. Feedback from the CMT will also be sought.

E7 Internal and external communications

General

E7.1 Managing communications, whether internally or externally, is a key aspect of crisis management. AIs should therefore have a coordinated approach to handling internal and external communications. To ensure that consistent messages are relayed, the same person (or team of persons) should be designated to handle all communication matters, including media relations and public announcements.

Internal communications

E7.2 To avoid chaos and confusion, the channels of internal communications should be managed during crisis management, with consistent information being disseminated to all relevant staff.

E7.3 When reporting information upward, some degree of information filtering and distillation will help ensure that only the key messages and the right degree of information required at each level of management should be relayed. Otherwise, management may encounter the problem of having too much information to digest or too little information upon which decisions are based.

E7.4 Sufficient support staff should be available to facilitate the recording (e.g. in the form of event logs, situation reports, etc.) and dissemination of information. This is necessary for effective management of the current situation and subsequent developments.

External communications

E7.5 Where possible, AIs should decide upon a media relations strategy from the start, including key messages which need to be communicated to external parties, and the most effective ways of doing this. There should however be flexibility for modifying the strategy to cater for changing circumstances.

E7.6 AIs should seek to be in a position of issuing information and explanations at the early stages of a crisis to quell any adverse publicity or speculative comments, but should ensure that such information is supported by solid evidence.

E7.7 There should be rigid controls to ensure that only authorized spokespersons can disseminate information through the media. Under a crisis, they could be the Chairman of the CMT and the Public Relations Manager. All press releases or prepared statements should be approved before issuance (with prior consultation with the HKMA).

E8 Pre-planning for crisis management

General

E8.1 Pre-planning is the key to successful crisis management, as there will be little time left during a crisis to start planning from scratch. Crisis management is therefore not limited to immediate management of crisis situations, but includes applying the same process to pre-planning how such situations may be handled.

E8.2 Although pre-planning gives AIs a chance to think ahead, it is impossible to pre-plan for all eventualities. Even the most detailed plans will not cover all possible combinations of circumstances. Flexibility should be built in, in order for AIs to cater for as many unforeseen circumstances as possible. Any pre-considered plans, or initial thought processes, should be reassessed in the light of the circumstances surrounding a real situation.

E8.3 All plans should be subject to regular tests and refinements to ensure their appropriateness. They should also be simple, concise and easy to comprehend.

E8.4 If a crisis situation is expected to cause business disruption (e.g. bank run, labour disputes resulting in industrial action, etc.), there are typically two types of plans, i.e. –

- plans to manage the situation itself; and
- plans to provide minimum essential business activities until full business recovery is achieved.

These plans will collectively allow an AI to manage a situation and to continue to function, although probably in a limited capacity.

E8.5 All personnel covered by these plans should be completely familiar with their contents. To facilitate easy reference, simple "checklists" or "reminder sheets" derived from the detailed plans may be used to ensure that the key decisions and tasks will not be missed.

Plans for managing specific crisis situations

E8.6 Detailed specific planning is difficult as the nature and circumstances of each crisis vary. As a result, the plans for managing specific crisis situations typically take the form of a checklist of generic tasks requiring consideration, with the focus being placed on –

- developing strategies and response actions for addressing stakeholder concerns and restoring, or minimising any damage caused to, an AI's reputation;
- formulating key messages to be communicated internally or with external parties (e.g. draft press statements);
- monitoring and reassessing the situation, and responding to changes; and
- where applicable, identifying business activities to be resumed or initiated as a matter of priority, and managing the business resumption process.

Plans for providing minimum essential business activities

E8.7 These plans deal mainly with the recovery of key business functions or processes, and not to provide business activities as usual (see TM-G-2 "Business Continuity Planning" for more guidance). The number of plans required will depend on the size and complexity of those functions or processes.