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 HKMA's supervisory approach to operational resilience and provide AIs with guidance on the general principles which they are expected to consider when developing their operational resilience framework.

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Previous guidelines superseded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. Definition of operational resilience
2. Operational resilience framework
3. Role of the Board and senior management
4. Determining operational resilience parameters
   - 4.1 Identifying critical operations
   - 4.2 Setting tolerance for disruption
   - 4.3 Identifying severe but plausible scenarios
5. Mapping interconnections and interdependencies underlying critical operations
6. Preparing for and managing risks to critical operations delivery
7. Testing ability to deliver critical operations under severe but plausible scenarios
8. Responding to and recovering from incidents

1. Definition of operational resilience

1.1 Operational disruptions (including those due to pandemics, cyber incidents, technology failures and natural disasters) can affect the viability of individual financial institutions, and in turn, the stability of the wider financial system. This underscores the significance of operational resilience as a supervisory focus and has motivated many regulators around the world and standard setting bodies to issue guidance that aims to improve the operational resilience of financial institutions.

1.2 The Principles for Operational Resilience (POR) issued by the Basel Committee on Banking Supervision (BCBS) in March 2021 defines operational resilience as the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption.

1.3 The HKMA expects all AIs in Hong Kong to be operationally resilient. The HKMA will consider an AI to be operationally resilient if it is able to satisfy the following requirements:

- Identify and mitigate risks that may threaten delivery of critical operations. In relation to an AI, **"critical operations"** refers to: (i) activities, processes and services performed by the AI, as well as (ii) the supporting assets (including people, technology, information and facilities) necessary for the delivery of such activities and services, which if disrupted, could pose material risks to the viability of the AI itself or impact the AI's role within the Hong Kong financial system[1].

[1] These should include any "critical financial functions", as defined in the Code of Practice "CI-1 Resolution Planning – Core Information Requirements", that may be performed by the AI.

- Continue to deliver critical operations when disruptions occur, including under severe but plausible scenarios. For this purpose, disruptions to an AI's critical operations must not exceed its **"tolerance for disruption"**, which is defined as the maximum level of disruption to a critical operation that an AI can accept, and is in practice the point after which further disruption would pose risks to the viability of the AI or impact its role within the Hong Kong financial system. **"Severe but plausible scenarios"** refers to situations that would result in significant disruptions, and while unlikely to occur, remain probable.
- Resume normal operations in a timely manner after disruptions occur; and
- Absorb learnings from disruptions or near-misses to continually improve its ability to prevent, adapt to and recover from risks and disruptions to critical operations delivery.

2. Operational resilience framework

2.1 An AI should develop an operational resilience framework which enables it to satisfy the requirements detailed in Section 1.3.

2.2 Given the importance of operational resilience for an AI to operate smoothly and remain viable under extreme scenarios, an AI's Board of Directors (Board) and senior management are expected to actively participate in establishing, implementing and overseeing the operational resilience framework.

2.3 At a minimum, an AI should include the following components within its operational resilience framework. Further guidance on how AIs may approach each of these components is provided in the subsequent sections of this module.

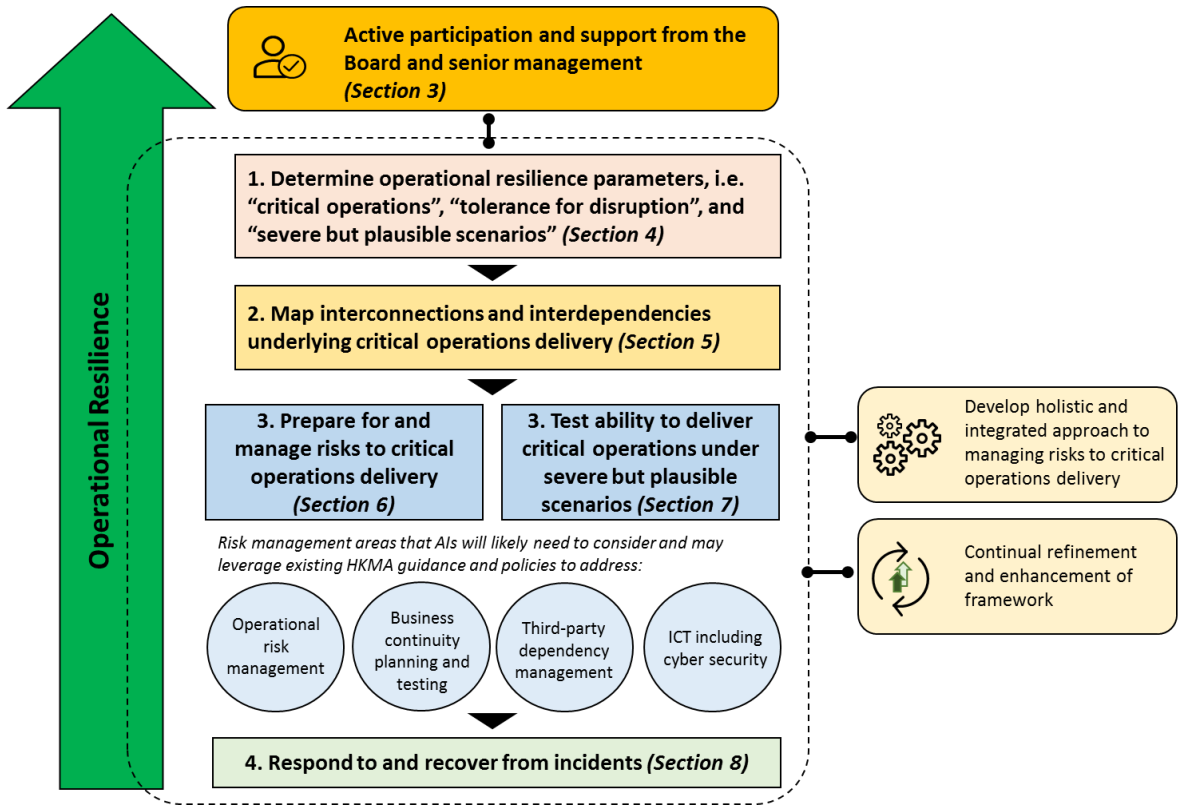
- Mechanism for determining the operational resilience parameters, namely critical operations, tolerance for disruption and severe but plausible scenarios. (Section 4)
- Mapping exercises which enable an AI to develop a detailed understanding of the interconnections and interdependencies that underlie critical operations delivery, and in turn, identify

what risks or events may affect or disrupt critical operations delivery. (Section 5)

- Risk management policies and frameworks that help an AI prepare for and manage the various risks to critical operations delivery in an integrated and holistic way. (Section 6)
- Scenario testing which enables an AI to regularly assess whether it is able to continue delivering critical operations through disruption, including under severe but plausible scenarios. (Section 7)
- An incident management programme which allows an AI to effectively respond to and manage disruptions to critical operations delivery. (Section 8)

2.4 An AI may determine the most appropriate approach to developing its operational resilience framework, taking into account its particular circumstances. AIs may refer to Diagram 1 for an illustration of how the different components can be brought together to create a holistic operational resilience framework. It is important to note that developing operational resilience is an iterative process. The process will not always be linear. An AI should actively apply learnings from its implementation of the framework and the management of actual incidents to continually improve on the effectiveness of the framework.

Diagram 1: Step-by-step approach to developing a holistic operational resilience framework



3. Role of the Board and senior management

3.1 The Board should be ultimately responsible for approving an AI's operational resilience framework and for overseeing its implementation. When formulating the framework, the Board should take into consideration the AI's risk appetite. For overseas incorporated AIs, this role should rest with the management team at the head office or the regional headquarters overseeing the Hong Kong operations of the AI.

3.2 Senior management should implement the operational resilience framework and ensure that sufficient resources (including financial, technological and otherwise) are allocated to this purpose. To facilitate the Board's oversight, senior management should provide regular and timely reports to the Board on the ongoing operational resilience of the AI's business units, particularly when significant deficiencies could affect the delivery of the AI's critical operations.

3.3 The Board and senior management should actively participate in the setting and review of an AI's operational resilience parameters. Specifically:

- The Board should approve and regularly review: (i) the criteria for determining an AI's critical operations; and (ii) the actual list of critical operations. The reviews should be conducted no less than annually or when major operational changes occur.
- The Board is responsible for setting the tolerance for disruption. Assisted by senior management, it should also review the tolerance for disruption at least on an annual basis or when major operational changes occur.
- Senior management should identify and the Board should approve the severe but plausible scenarios which will be used to review whether an AI is operationally resilient. Both the Board and senior management should regularly review the continued relevance of the scenarios identified.

3.4 The Board bears ultimate responsibility for ensuring that an AI remains operationally resilient. This would require the Board to take appropriate action to address any deficiencies identified in an AI's ability to remain within its tolerance for disruption. In the event that there is more than one source of deficiency, the Board should suitably prioritise the remedial actions. As a general principle, the Board should place its focus on making improvements to those areas that would result in larger disruptions, higher risks or are facing more significant deficiencies. For instance, an AI should prioritise a critical operation that would more sooner breach its tolerance for disruption over one that is less time sensitive, or a critical operation that is further away from remaining within its tolerance for disruption over one that is largely within its tolerance for disruption.

3.5 The Board and senior management should regularly review the suitability and effectiveness of the AI's operational resilience framework. These reviews are particularly important following operational changes and during the transitory period after an

operational change comes into effect.

3.6 The Board should play an active role in establishing a broad understanding of the AI's operational resilience framework. It should clearly communicate the objectives of the framework to all relevant parties, including staff, intragroup entities and third parties. Regular training on the AI's operational resilience framework should be provided to these parties to reinforce their understanding.

4. Determining operational resilience parameters

4.1 Identifying critical operations

4.1.1 As a first step to developing a sound operational resilience framework, an AI should identify its critical operations. The number of critical operations identified should be commensurate with the size, nature and complexity of the AI's operations.

4.1.2 When identifying its critical operations, an AI should take into consideration a set of defined criteria. These criteria should allow an AI to critically assess whether an operation, if disrupted, would affect:

(a) The AI's viability. Possible factors to consider include the impact on customers and personnel, and financial, reputational, legal and regulatory implications.

(b) The AI's role in the Hong Kong financial system. Possible factors to consider include how disruptions may affect specific market roles played by the AI (e.g. note issuance or clearing) as well as relationships with counterparties in the interbank market.

For the avoidance of doubt, while the set of criteria defined by AIs for identifying critical operations should encompass elements of both (a) and (b) above, a given operation need not impact both (a) and (b) in order for it to be classified as a critical operation.

4.1.3 In the process of identifying its critical operations, an AI may, where appropriate, leverage on relevant concepts covered within its recovery and resolution plans.

4.2 **Setting tolerance for disruption**

4.2.1 A tolerance for disruption should be set for each critical operation. It should include at least a time-based metric, but may also include a combination of other quantitative (e.g. volume or value of transactions) and qualitative metrics (e.g. reputational or legal implications).

4.2.2 In setting the tolerance for disruption, consideration should be given to an AI's operational capabilities given a broad range of severe but plausible scenarios that would affect its critical operations. AIs should be aware that their operational capabilities may vary during different business cycles or as a result of seasonal factors. For instance, during the periods of time when more initial public offerings are launched, an AI's trading systems are more likely to come under stress, which could weaken the AI's ability to respond under severe but plausible scenarios.

4.3 **Identifying severe but plausible scenarios**

4.3.1 AIs should identify a range of scenarios of different nature, severity and duration relevant to its business and risk profile. Examples of scenarios that AIs may consider include, but are not limited to, pandemics, natural disasters, and failures or disruptions at a third party or within the third party's supply chain.

4.3.2 When identifying the scenarios, AIs should make reference to previous incidents or near misses within the institution or across financial sectors, as well as in other sectors or jurisdictions, or any situations that could result in significant disruptions given the changing operational landscape.

5. Mapping interconnections and interdependencies underlying critical operations

5.1 The appropriate functions within an AI should identify and document: (i) the people, processes, technology, information, facilities; and (ii) the interconnections and interdependencies among these factors that are necessary for the AI to deliver its critical

operations. When considering (ii), an AI should also include those interconnections and interdependencies that depend on third parties and intragroup arrangements.

5.2 The approach and level of granularity of mapping should be sufficient to enable the AI to identify vulnerabilities and facilitate the testing of the AI's ability to deliver critical operations through disruptions. AIs should also consider whether the approach adopted for mapping under its operational resilience framework is appropriately harmonised with that adopted for recovery and resolution planning purposes.

5.3 The mapping documentation should be prepared in a way that is proportionate to the AI's size, scale and complexity. It should also be usable by all relevant parties in the event of disruptions.

5.4 AIs are expected to update their mapping documentation on a regular basis, but no less than annually or following any material changes to their operations.

6. Preparing for and managing risks to critical operations delivery

6.1 AIs should be prepared to manage all risks with potential to affect critical operations delivery. As a given critical operation may face a number of risks, AIs should leverage different risk management frameworks, as appropriate, to offer holistic and comprehensive support to the critical operation.

6.2 The HKMA expects that AIs should, at a minimum, take into consideration the following risk management components with respect to operational resilience:-

- Operational risk management: As operational risk management focuses on preventing and minimising operational losses, it contributes to an AI's efforts to maintain operational resilience. Operational risk management should therefore be considered as a crucial element of an effective operational resilience framework.
- Business continuity planning and testing: Business continuity planning and testing supports an AI's ability to prepare for and

recover from emergencies or disasters, and therefore contributes to an AI's ability to continue delivering its critical operations through disruptions. Accordingly, AIs should ensure that their critical operations are subject to appropriate business continuity planning and testing arrangements.

- Third-party dependency management: As AIs increasingly engage third parties or intragroup entities for the provision of services or delivery of functions, they must ensure that disruptions at these entities will not affect critical operations delivery. To ensure potential risks to critical operations are minimised, AIs should manage their dependencies on third parties and intragroup entities as they would with outsourcing arrangements. Prior to entering into arrangements that support the delivery of critical operations, an AI should verify whether the relevant third parties or intragroup entities have at least equivalent level of operational resilience to that of the AI. During the course of engagement, an AI should have adequate arrangements in place to continually satisfy itself that the third party or intragroup entity has maintained an acceptable level of operational resilience. In addition, an AI should develop appropriate business continuity and contingency planning procedures and exit strategies to maintain its operational resilience in the event of a failure or disruption at a third party or intragroup entity which may impact its delivery of critical operations. An AI should not enter into, or continue, any third party or intragroup arrangements that may weaken the operational resilience of the AI's critical operations.
- Information and Communication Technology (ICT) including cyber security: Growing technology adoption raises the likelihood that an AI's critical operations may depend or may be affected by lapses in ICT risk management. To minimise risks in this regard, AIs should have in place an ICT policy which covers cyber security, as well as arrangements for ensuring the confidentiality, integrity and availability of critical

information assets.

6.3 AIs should note that most of the risk management considerations associated with operational resilience are not new, and are already covered by existing HKMA guidance. These include but are not limited to: Supervisory Policy Manual (SPM) modules "TM-G-1 General Principles for Technology Risk Management", "TM-G-2 Business Continuity Planning", "OR-1 Operational Risk Management", "SA-2 Outsourcing", as well as "Cyber Resilience Assessment Framework 2.0". AIs should refer to and ensure that they are compliant with the supervisory requirements contained therein.

7. Testing ability to deliver critical operations under severe but plausible scenarios

7.1 AIs should conduct regular testing of their operational resilience framework to ensure that they are able to continue delivering their critical operations through disruptions, including under severe but plausible scenarios.

7.2 When considering the testing requirement, AIs should take into account the following:

- The testing exercises should include realistic assumptions, and should encompass the AI's interconnections and interdependencies, including those through relationships with intragroup entities and third parties.
- The frequency of testing should be determined based on a variety of factors, including the potential impact of a disruption, how many critical operations an AI has, and whether the operating environment has materially changed.
- Different types of testing (e.g. paper-based, simulations or live-systems testing) serve different purposes and AIs should deploy the most appropriate type of testing based on the nature or needs of the specific testing exercise. An AI should also consider and carefully manage the risks that may be introduced by the testing itself.
- AIs should deploy staff with appropriate expertise to conduct

the testing. The testing approach should dictate the type of staff involved, including their seniority, qualifications as well as the function (e.g. first, second or third line of defence) from which they are sourced.

- AIs should consider how they may leverage the testing exercises to enhance their staff's operational resilience awareness and readiness to operate during disruptions, thereby improving their ability to effectively adapt and respond to different types of disruptive events.

7.3 Where practicable, AIs may leverage on existing testing arrangements, including those devised for business continuity planning purposes, to fulfill the testing requirement relating to operational resilience. An AI should be able to demonstrate how an existing testing exercise enables it to achieve the specific objectives of scenario testing for operational resilience purposes.

7.4 After each testing exercise, an AI should prepare a formal testing report to record any gaps or weaknesses identified, as well as document the remedial actions planned. The reports should be reviewed by the AI's senior management.

8. Responding to and recovering from incidents

8.1 While an AI should dedicate adequate efforts to preventing disruptions, it should recognise that disruptions will occur no matter how robust its operational resilience framework is. An AI should therefore be prepared to manage and recover from incidents.

8.2 Specifically, an AI should establish an effective incident management programme to manage all incidents, especially those that may impact its critical operations. The programme should cover those incidents that may arise due to dependencies, including those on third parties and intragroup entities.

8.3 The incident management programme should capture the full life-cycle of any incidents and involve:

- Classification of an incident's severity based on predefined criteria. This should enable the AI to prioritise and allocate resources to respond to an incident.

- Incident response and recovery procedures. These should be reviewed, tested and updated on a regular basis. Their connection to the AI's business continuity, disaster recovery and other associated management plans and procedures should also be clearly documented.
- Communication plans for reporting incidents to both internal and external stakeholders. Communication should take place during the incident (e.g. to provide performance metrics), and after, including to convey analysis of lessons learned.
- Root cause analysis of incidents to help with the prevention or minimisation of recurrence.

8.4 The incident management programme should be supported by an inventory of internal and third party resources to enable prompt incident response and recovery. It should also reflect the lessons learned from previous incidents, including those experienced by others.

8.5 AIs should note that the above requirements complement existing HKMA guidance on incident management. These include but are not limited to SPM modules "TM-G-2 Business Continuity Planning" and "TM-G-1 General Principles for Technology Risk Management", and the HKMA's circular on "Incident Response and Management Procedures" issued in June 2010. AIs should review relevant materials and ensure that they are compliant with the supervisory requirements contained therein.

9. Implementation of operational resilience requirements

9.1 Application

9.1.1 The requirements contained in this module apply to all AIs. Locally incorporated AIs should endeavour to implement the guidance of this module with respect to their subsidiaries and overseas operations, and for overseas incorporated AIs with respect to their operations in Hong Kong.

9.1.2 In line with the HKMA's risk-based approach to supervision, AIs are expected to implement the requirements in a

proportionate manner and develop an operational resilience framework that is "fit for purpose", i.e. commensurate with its nature, size, complexity and risk profile.

9.2 **Timeline for implementation**

9.2.1 By [1 year after the date upon which the final module is issued], the HKMA expects an AI to have:

(a) Developed its operational resilience framework; and

(b) Determined the timeline by which it will have implemented the operational resilience framework, and become operationally resilient.

9.2.2 For the purposes of 9.2.1(a), AIs are expected to have identified the operational resilience parameters and commenced a basic programme of mapping. The latter will be crucial to ensuring that an AI adequately understands the interconnections and interdependencies that underlie its critical operations, and in turn, is able to develop the other components of its operational resilience framework, including to identify the specific types of risks to critical operations delivery that need to be addressed, as well as how to most suitably conduct testing. The HKMA recognises that AIs may not be able to produce mapping that reaches the full level of sophistication at the initial stage, and instead, would expect AIs to make continual improvements as they obtain more experience in implementing their operational resilience frameworks.

9.2.3 Given the importance of operational resilience, the HKMA expects AIs to become operationally resilient as soon as practicable. That said, the HKMA also recognises that becoming operationally resilient is a resource-intensive exercise (for reasons including that it involves mapping exercises which may be more complex for larger AIs, and could involve substantial system changes). Taking into consideration the need to accommodate AIs of different size and complexity, the HKMA has decided to allow AIs up to 2 years to become operationally resilient. In other words, the

timeline specified under Section 9.2.1(b) should not extend beyond 2 years from [1 year after the date upon which the final module is issued.] After this point in time, an AI will be expected to have fully implemented its operational resilience framework, including to have conducted scenario testing, and be able to satisfy the requirements in Section 1.3. Notwithstanding the 2-year time limit, AIs are encouraged to become operationally resilient as soon as their circumstances allow. The HKMA will engage in active discussions with AIs to review the suitability of their proposed timelines.

9.3 Supervisory approach

9.3.1 Following its risk-based supervisory approach, the HKMA will assess the effectiveness of the operational resilience frameworks of AIs through a combination of risk-focused on-site examinations, off-site reviews and prudential meetings. Where needed, AIs may be required to submit self-assessments of their ability to remain operationally resilient.

———————————