

## **Good practices for mapping interdependencies and scenario testing**

This annex summarises a set of good practices for mapping interdependencies and scenario testing noted by the HKMA over the course of its supervision of AIs' implementation of their operational resilience frameworks.

### **A. Governance**

#### 1. Ensure effective oversight of implementation of operational resilience framework including the mapping and scenario testing exercises

The Board and senior management exercise effective oversight of the implementation of operational resilience framework by embedding operational resilience as one of the intended outcomes into their strategic planning, risk management and business/product approval processes.

The senior management of major AIs has established clear accountability and designated an owner for each critical operation to lead the end-to-end mapping and scenario testing exercises. Some AIs have established a cross-departmental group to draw specialist resources, including risk management experts, business continuity specialists and IT security professionals, in conducting the mapping and testing processes.

In some AIs, the senior management challenges the owner of a critical operation by playing out the scenario of failure of specific underlying assets and requesting the owner to provide impact assessment and response plans. Self-assessments are conducted and regular reporting is made to the Board on the implementation progress of the operational resilience framework.

### **B. Mapping**

#### 2. Define the start and end points of a critical operation to facilitate the mapping of the underlying assets

As part of the planning process, major AIs have identified the start and end points of a critical operation to establish a clear scope for mapping. Some AIs take into account the business process flow, customer journey and IT

dependencies in defining the end-to-end critical operations. Decision points for continuing the business-as-usual paths and triggering alternative paths for contingency are identified. Interdependencies of the critical operation with any upstream and downstream systems, as well as communication and data exchange between relevant parties, are also captured. These enable the identification of all supporting assets (people, processes, technology, information, facilities, and interconnections and interdependencies) necessary for the delivery of a critical operation.

3. Adopt appropriate tools to construct a comprehensive map

Major AIs utilise the information in their existing risk management frameworks, such as business impact assessments (BIAs), risk and control assessments, IT service chain map, network diagrams and inventory of third-party service providers, to capture the known critical supporting assets in the map. Some AIs have also developed a template or guidance note to set out the procedures required for the delivery of critical operation, supporting staff and their functions, physical sites and their alternate locations, system owners, system hosting locations, and recovery time objectives. These details serve as a basis for the development of a comprehensive map and identification of dependencies, ensuring comprehensive coverage of supporting assets in the map.

4. Identify vulnerabilities taking a risk-based approach in the end-to-end map

Based on the preliminary map constructed, critical operation owners would conduct an end-to-end review to identify points that are susceptible to disruption or single point of failure. This is achieved through analysing the data and process flows, conducting technology resilience reviews or by analysing real-life disruptions. It also involves examining the potential impact of different third-parties' failure to a critical operation.

Additionally, some AIs consider emerging risks by assessing the impact of large-scale global incidents on different types of critical operation, and whether similar supporting assets within the critical operation are prone to disruptions, thereby enabling the identification of vulnerabilities in a forward looking manner.

5. Establish trigger events for revisiting the map to capture emerging risks

In addition to conducting regular reviews of the mapping results, major AIs have defined a number of trigger events for updating the map to capture emerging risks and to ensure the mapping results remain effective in identifying vulnerabilities. Examples of such events include real-life disruptions, observations from regular risk assessments, and changes to third-party support for critical operations. For instance, some AIs would incorporate dependencies and vulnerabilities revealed by an incident into the critical operation map, and incorporate lessons learnt into their operational resilience frameworks. Furthermore, some AIs have engaged independent parties, such as the second or third line of defence or external consultants, to review and provide feedback on the mapping results (e.g. reasonableness of the vulnerabilities identified), with a view to enhancing the quality of mapping at an early stage.

6. Access to mapping documentations

Many AIs have developed a critical operation-specific manual or a centralised repository to enable all relevant parties to access a single source of up-to-date mapping documentation during business-as-usual or in the event of disruptions. Mapping documentation may comprise an end-to-end view of resilience across the supporting assets of a critical operation (e.g. a flow chart covering the business-as-usual paths and alternative paths for contingency), vulnerabilities associated with a critical operation, lessons learnt from testing, triggering events for reviews, remedial measures implemented, and scenario-based response and recovery processes. Workflow systems are also utilised to record mapping results at a sufficiently granular level, facilitating the monitoring of mapping status and updates of emerging risks.

**C. Scenario Testing**

7. Establish an effective test plan with clear objectives

The test plans of major AIs have a clear overarching objective, which is to assess whether a critical operation can be delivered within the tolerance for disruption. Building on the overarching objective, some AIs also established more granular and targeted objectives, allowing them to better assess under what conditions (e.g. reduced manpower, manual workaround) the tolerance

for disruption might be breached, so as to overcome the constraints hindering recovery.

Given that it is not possible to test all severe but plausible scenarios for all critical operations at once, major AIs have developed a systematic test plan that takes into account emerging risks and impacts of vulnerabilities. Vulnerabilities that impact multiple critical operations are given the highest priorities. This enables the proper prioritisation and sequencing of the various tests, while ensuring appropriate coverage of each critical operation under each severe but plausible scenario. For instance, some AIs repeatedly tested payment operations due to prior disruptions in these operations, while others prioritised testing of critical operations involving third parties, considering the rising instances of major disruptions caused by third parties.

#### 8. Adopt an outcome-based testing approach

Once the test objectives are established, many AIs would determine the most suitable type of testing, considering the distinct objectives served by different types of tests. To assess whether a critical operation can be delivered within the tolerance for disruption, major AIs adopted various types of tests in isolation or in combination, including scenario tests (e.g. ransomware attack, third-party disruption, system failure), business continuity tests, simulation exercises (e.g. core banking system migration impacting multiple critical operations), and disaster recovery tests (e.g. loss of data centre). Some of them utilise a paper-based format to facilitate more thorough validation of recovery procedures and their operability, while others employ a table-top format, which enables the testing of real-time responses from relevant parties within a condensed timeframe.

#### 9. Design dynamic and stressful testing scenarios to simulate potential disruptions

In designing a testing scenario, some major AIs would increase the severity of disruption over time with a view to testing the AI's tolerance limit and identifying vulnerabilities under stressed situations. Some AIs also developed a storyline to simulate the different stages of a real-life disruption (e.g. limited information on the outage of a critical third-party service provider initially, followed by more updates on the root cause and impacts at a later stage). Sub-storylines are also included to illustrate the need to involve relevant stakeholders as the disruption starts to impact more lines of business (e.g. IT

team fixes payment processing system slowness, while the payment team initiates manual operation as the issue persists). Furthermore, more mature AIs would combine multiple severe but plausible scenarios to create even more stressful assumptions, such as concurrent disruptions from multiple sources impacting the same critical operation.

10. Engage appropriate stakeholders (including third parties and intragroup arrangements) in the testing exercise

Some AIs involve the senior management of their external system vendors in planning and conducting the testing exercise on whether the vendors' tolerance limit is within the AIs' tolerance level in respect of a particular critical operation. Some AIs engage their intragroup functions to ensure that the intragroup arrangements are effective in supporting the continuous delivery of critical operations. AIs that face challenges in engaging third parties in scenario testing have adopted alternative approaches to assess third-party resilience, such as reviewing their resilience plans and testing outcomes. Where such information is limited or unavailable, the AIs concerned would assume that the third party did not meet their resilience requirements, identify this as a gap, and review whether substitutes or workarounds are available.

11. Evaluate testing results to identify areas for improvement and refine testing approach to enhance effectiveness

Major AIs evaluate their testing results and continually refine their testing approach to more effectively uncover potential vulnerabilities. This process involves a thorough evaluation of testing results, carefully examining the underlying assumptions to identify gaps and weaknesses. For example, some AIs have refined their testing approach or adjusted their assumptions, such as transitioning from a paper-based to a table-top exercise, or performing live system tests from weekends to weekdays. Some AIs retested the scenarios to track improvements over their vulnerabilities.

**D. Remediation of vulnerabilities**

12. Manage vulnerabilities for remediation

Major AIs have made progress in remediating vulnerabilities identified ahead of 31 May 2026. This is achieved by assessing the impact of vulnerabilities on single or multiple critical operations and making prioritisation accordingly.

Additionally, some AIs classify vulnerabilities in different tiers to formulate a suitable remedial strategy, seek appropriate funding and continuously track remediation progress.

Some AIs established dashboards to track different types of vulnerabilities and remediation, as well as introducing heat maps to track operational resilience posture. This involves recording whether each critical operation could remain within the defined tolerance for disruption under each severe but plausible scenario. Taking into account any vulnerabilities being addressed throughout a period, the dashboards and heat maps are also updated to reflect the latest remediation status and operational resilience posture. Periodic reporting of all vulnerabilities is made to risk committees and other governance parties.

### 13. Derive suitable remediation strategy

Major AIs have formulated suitable strategies in line with the type and nature of vulnerabilities identified. For instance, AIs remediated their technology-related vulnerabilities by tightening recovery timeframes, enhancing requirements for technology-related tests, and acquiring additional recovery capacity. In other cases, AIs with data-related vulnerabilities revisited the recovery timeframe for their Secure Tertiary Data Backup (STDB) to ensure it is within the tolerances for disruption. Meanwhile, certain AIs with process-related vulnerabilities have enhanced their manual processes by refining the scenario-based response and recovery plans to support the delivery of critical operations.