

CONSULTATION PAPER

P015 - 2021
October 2021

Second Consultation Paper and Response to Feedback Received on Proposed Revisions to Guidelines on Business Continuity Management

MAS

Monetary Authority of Singapore

Contents

1	Preface	3
2	Proposed Revisions to Guidelines on BCM	4
3	ANNEX A – List of Questions	10
4	ANNEX B – Revised Guidelines on BCM	11
1	Introduction	11
2	Critical Business Services and Functions.....	14
3	Service Recovery Time Objective.....	16
4	Mapping of Interdependencies	17
5	Concentration Risk.....	19
6	Continuous Review and Improvement	21
7	Testing	23
8	Audit	25
9	Crisis Management and Communications	26
10	Responsibilities of Board and Senior Management	28
	Appendix: Examples of Business Service	31
5	ANNEX C – Response to Feedback Received from First Consultation Paper.....	32

1 Preface

1.1 The Monetary Authority of Singapore (MAS) issued a consultation paper on Proposed Revisions to Guidelines on Business Continuity Management (BCM) (hereafter referred as “the Guidelines”) in 2019.

1.2 MAS would like to thank all respondents who provided feedback and comments for the earlier consultation. This second consultation builds on feedback received from the first consultation, along with key learnings from the COVID-19 pandemic.

1.3 Financial Institutions (FIs) will be expected to adopt the Guidelines within a year following the publication of the revised Guidelines. The revised Guidelines will supersede BCM Guidelines published in June 2003 and MAS Circular SRD BCM 01/2006. MAS invites interested parties to submit their views and comments on the Guidelines. All comments should be submitted to MAS by 15 November 2021.

1.4 **Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like (i) their whole submission or part of it (but not their identity), or (ii) their identity, or both, to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.**

1.5 Electronic submission via [online submission form](#) is encouraged. If you have any queries, please email bcp@mas.gov.sg.

2 Proposed Revisions to Guidelines on BCM

2.1 The following sets out the key changes to the existing Guidelines on BCM.

Critical Business Services and Functions

2.2 Business functions underpin the provision of business services to an FI's customers. A business function could also concurrently support a few different business services provided by the FI. When such a business function is disrupted, all the business services that are dependent on it could be disrupted, and as a result, amplify the operational or business impact to the FI. An FI may also have business functions that do not directly contribute to a business service, such as IT support and human resource, but could impact the FI's safety and soundness if disrupted.

2.3 In the event of a disruption, it might not be practical nor possible to recover all business services and functions at the earliest opportunity due to time and resource constraints. FIs should therefore prioritise the recovery of its business services and functions based on their criticality to determine the appropriate recovery strategies and resource allocation.

2.4 FIs should identify their critical business services (refer to **Appendix: Examples of Business Services**) and functions¹ by considering the impact of their unavailability on:

- (a) the FI's safety and soundness;
- (b) the number and profile of customers affected; and
- (c) the FI's counterparties and other participants in the financial ecosystem.

2.5 In establishing recovery strategies, FIs should adopt an end-to-end view of the critical business services' dependencies, to not only consider the recovery of individual processes, but the complete set of processes supporting the delivery of the service. This will minimise the degree of disruption, safeguard customer interests, and maintain the safety and soundness of FIs.

¹ An FI can adopt the business impact analysis methodology to assist in its identification of critical business services and functions.

2.6 FIs should also ensure clear accountability and responsibility for the overall business continuity of each critical business service. Where the delivery of a business service depends on multiple business functions, an overall manager should be appointed to coordinate incident management across the affected functions, and oversee the resumption of the business service in the event of a disruption.

Question 1. MAS seeks comments on the proposed identification and prioritisation of critical business services in addition to critical business functions.

Service Recovery Time Objective

2.7 FIs should establish the **Service Recovery Time Objective (SRTO)** for each critical business service. The SRTO, being a time-based metric, provides clarity between FIs and their third parties on the recovery expectation of the business service. This will help to facilitate decision-making and monitoring of the progress of its recovery following a disruption.

2.8 In establishing SRTOs, FIs should take into consideration its obligations to customers, the financial ecosystem, and its participants. FIs are expected to put in place recovery strategies² to enable them to achieve the established SRTOs and recover to the service levels required to meet their business obligations. For critical business services that are supported by a number of business functions, FIs must ensure that the Recovery Time Objectives (RTOs) of the underlying business functions and their dependencies will meet its SRTOs.

2.9 FIs should also set out clear and defined thresholds for BCP activation in the event where the performance of a critical business service is reduced or intermittent, but not to the extent that it is completely unavailable. This will guide the FI in activating its BCP in a timely manner, before the performance degradation becomes overly prolonged or worsened to the extent that it results in severe impact.

Question 2. MAS seeks comments on the proposed establishment of Service Recovery Time Objectives (SRTO) for each critical business service, and the implementation of recovery strategies to meet the SRTOs.

² Examples of recovery strategies could include manual workarounds, activation of alternate sites, and expansion of the service capacity of alternate delivery channel(s) to meet the increase in demand.

Mapping of Interdependencies

People, Processes and Technology

2.10 The financial sector has become increasingly interconnected with the growing reliance on IT systems and common third parties. As a first step to mitigate the risks arising from the interdependencies, FIs should identify and map the end-to-end dependencies on people, processes, and technology, including those involving third parties, that support each critical business service.

2.11 The dependency mapping will enable FIs to identify resources critical to the service delivery, consider the implications of their unavailability, and address any gaps that could hinder the effectiveness and safe recovery of the critical business services. FIs should use the information derived from the dependency map to verify that the recovery of the business functions and their dependencies, will meet the established SRTOs.

Third Party Dependencies

2.12 Most FIs engage third parties³ to support the delivery of their critical business services. These arrangements could increase operational risk arising from the failure, delay, or compromise of a third party in providing the service.

2.13 The FI should perform its due diligence to obtain assurance that the SRTOs of the critical business service can be met by the third parties. This assurance can be obtained through measures, such as the following, where possible:

- (a) Establish and regularly review operational level or service level agreements with third parties that set out specific and measurable recovery expectations;
- (b) Request for dedicated manpower from their third party service providers for specialist functions that cannot be performed in-house; or
- (c) Conduct audits, regular tests, or joint tests with their third parties to ensure that the third parties have the ability to support FIs even in the scenario that these third parties experience disruptions.

³ These include third party service providers as well as intra-group service providers.

2.14 FIs should also put in place plans and procedures⁴ to manage and address any unforeseen disruption, failure or termination of third party arrangements to minimise the impact of such adverse events on their business continuity.

2.15 Some interdependency risks (e.g. unavailability of telecommunications networks, power utilities, etc.) may be beyond an FI's direct control to mitigate completely. Hence, it is important that FIs put in place risk mitigating measures, such as implementing redundancy or back-up arrangements, to address the interdependency risks posed by the disruption of these services.

Question 3. MAS seeks comments on the proposed development of an end-to-end dependency mapping on people, processes, and technology, including those involving third parties, for each critical business service.

⁴ Examples include pre-designating an alternate service provider or building up in-house capability in the event where the primary service provider is unavailable to provide immediate support.

Audit

2.16 A BCM audit is an important means to provide the FI with independent assessment on the adequacy and effectiveness of the implementation of the FI's BCM framework. An FI should ensure that its audit programme adequately covers the assessment of BCM preparedness based on the level of operational risks that it is exposed to.

2.17 The scope and frequency of BCM audits⁵ should be commensurate with the criticality of the business services and business functions. The BCM audits should be conducted by a qualified independent party (e.g. qualified internal or external auditor).

2.18 The FI should establish processes to track and monitor the implementation of remedial actions in response to the audit findings. FIs should escalate any significant audit findings on lapses that may have severe impact on the FI's BCM to the Board and senior management. The FI should submit the BCM audit reports to MAS upon request.

2.19 Please see **Annex B** for the proposed revised Guidelines on BCM.

Question 4. MAS seeks comments on the expectation to conduct BCM audits that are commensurate with the criticality of the business services and functions.

Question 5. MAS seeks comments on any other aspects of BCM that warrant further guidance from MAS.

⁵ Examples of BCM audits include institutional-wide BCM audits, specific service or function-level audits covering BCM preparedness, or thematic audits.

3 ANNEX A – List of Questions

- Question 1.** MAS seeks comments on the proposed identification and prioritisation of critical business services in addition to critical business functions. 5
- Question 2.** MAS seeks comments on the proposed establishment of Service Recovery Time Objectives (SRTO) for each critical business service, and the implementation of recovery strategies to meet the SRTO. 6
- Question 3.** MAS seeks comments on the proposed development of an end-to-end dependency mapping on people, processes, and technology, including those involving third parties, for each critical business service. 8
- Question 4.** MAS seeks comments on the expectation to conduct BCM audits that are commensurate with the criticality of the business services and functions. 9
- Question 5.** MAS seeks comments on any other aspects of BCM that warrant further guidance from MAS. 9

4 ANNEX B – Revised Guidelines on BCM

1 Introduction

Preface

1.1 The proper functioning of the financial sector is underpinned by trust and confidence in the financial ecosystem’s ability to protect assets and transactions. Operational disruptions, if not recovered speedily, may compromise the ability of financial institutions (“FIs”) to meet their business obligations and result in significant financial losses. Given the high interconnectedness between FIs, these disruptions, if severe and widespread, may even lead to broader contagion implications for the financial system.

1.2 MAS is concerned with both the soundness of individual FIs, and the stability of the financial system as a whole. To that end, FIs are expected to have controls in place to minimise the occurrence of operational disruptions, including identifying potential single points of failure early on and eliminating them, where possible.

1.3 MAS also recognises that disruptions could, nevertheless, still occur despite an FI’s best efforts. An effective Business Continuity Management (BCM) framework will therefore be critical in minimising the impact of operational disruptions on an FI’s ability to continually deliver financial services.

1.4 Having a sound BCM framework enables an FI to responsively harness the three elements – people, processes, and technology – to recover from operational disruptions. The COVID-19 pandemic, as a case in point, saw lockdowns and the implementation of safe management measures that restricted the mobility of resources and resulted in the wider adoption of remote working arrangements. Despite these restrictions, many FIs were able to continue meeting their business obligations as they had a comprehensive BCM framework in place.

1.5 BCM is an ongoing effort to ensure that the plans and procedures put in place are able to address operational risks posed by the latest threats. FIs should adopt a proactive BCM posture by embedding BCM into their business-as-usual operations and processes, and contribute to the overall operational resilience of the financial sector.

1.6 MAS has issued this revised set of BCM Guidelines to share best practices and to reinforce the importance of having an over-arching BCM framework in place to ensure FIs’ operational resilience.

Application of Guidelines

1.7 The set of MAS BCM Guidelines (hereafter referred to as “the Guidelines”) contains sound BCM principles that FIs are encouraged to adopt to strengthen their resilience against operational disruptions. FIs should establish policies, plans and playbooks to maintain an FI’s business continuity preparedness, and ensure that its critical business services can be promptly resumed following a disruption.

1.8 FIs are ultimately responsible for their own business continuity preparedness and recovery from operational disruptions. MAS expects FIs to have robust business continuity plans (BCPs) that address a range of severe and plausible disruption scenarios. The extent and degree to which an FI implements the Guidelines should be commensurate with the nature, size, and complexity of its business operations. FIs may adapt the Guidelines as necessary, taking into consideration the diverse activities they engage in, and the different markets in which they conduct transactions.

1.9 In supervising an FI, MAS will review the FI’s BCM, taking into account the extent to which the FI observed the Guidelines, to assess the quality of its oversight and governance arrangements, internal controls, and risk management. Particular attention will be paid to business continuity policies, plans and playbooks established for an FI’s critical business services.

1.10 FIs’ senior management and personnel, who are responsible for implementing BCM, should familiarise themselves with the Guidelines and understand the intent and implications of the Guidelines. This document provides general guidance, and is not intended to be exhaustive nor replace or override any legislative provisions. It should be read in conjunction with the provisions of the relevant legislations, the subsidiary legislations made under the relevant legislations, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislations and subsidiary legislations.

1.11 This set of Guidelines supersedes the previous version that was published in June 2003, as well as the circular titled “Further Guidance on BCM” that was issued in January 2006.

1.12 The Guidelines is applicable to all FIs as defined in Section 27A(6) of the Monetary Authority of Singapore Act. It will not apply to overseas subsidiaries and branches of the FI.

Glossary

Terminology	Definitions (as used in this document)
Business Continuity Management (BCM)	A set of practices that includes putting in place policies, standards, processes, and measures to provide for continuous functioning of the FI during operational disruptions. It should be commensurate with the FI's nature, size, and complexity of business activities.
Business Continuity Plan (BCP)	A plan that sets out the (1) roles and responsibilities, (2) resources, and (3) processes that are needed to recover and fulfil the FI's business obligations following an operational disruption, and restore its operations to normalcy.
Business Function	An activity or set of activities performed by individual organisational lines (i.e. department or unit) in the FI.
Business Service	An external-facing service that is provided to customers of an FI.
Critical Business Function	A business function which, if disrupted, is likely to have a significant impact on an FI, whether financially or non-financially.
Critical Business Service	A business service which, if disrupted, is likely to have a significant impact on the FI's safety and soundness, or its customers or other participants of the financial ecosystem.
Dependency Mapping	A process to identify and understand the internal and external dependencies on people, processes, and technology for each critical business service.
Recovery Time Objective (RTO)	Target duration of time to restore a specific <i>business function</i> from the point of disruption, to the point when the specific <i>business function</i> is recovered to a level sufficient to meet business obligations.
Service Recovery Time Objective (SRTO)	Target duration of time to restore a specific <i>business service</i> from the point of disruption, to the point when the specific <i>business service</i> is recovered to a level sufficient to meet business obligations.
Recovery Strategy	A clear, defined, and tested course of action to be taken in response to operational disruptions.

2 Critical Business Services and Functions

2.1 Business functions underpin the provision of business services to an FI's customers. A business function could also concurrently support a few different business services provided by the FI. When such a business function is disrupted, all the business services that are dependent on it could be disrupted, and as a result, amplify the operational or business impact to the FI. An FI may also have business functions that do not directly contribute to a business service, such as IT support and human resource, but could impact the FI's safety and soundness if disrupted.

2.2 In the event of a disruption, it might not be practical nor possible to recover all business services and functions at the earliest opportunity due to time and resource constraints. FIs should therefore prioritise the recovery of its business services and functions based on their criticality to determine the appropriate recovery strategies and resource allocation.

2.3 FIs should identify their critical business services (refer to **Appendix: Examples of Business Services**) and functions⁶ by considering the impact of their unavailability on:

- (a) the FI's safety and soundness;
- (b) the number and profile of customers affected; and
- (c) the FI's counterparties and other participants in the financial ecosystem.

2.4 In establishing recovery strategies, FIs should adopt an end-to-end view of the critical business services' dependencies, to not only consider the recovery of individual processes, but the complete set of processes supporting the delivery of the service. This will minimise the degree of disruption, safeguard customer interests and maintain the safety and soundness of FIs.

2.5 FIs should also ensure clear accountability and responsibility for the overall business continuity of each critical business service. Where the delivery of a business service depends on multiple business functions, an overall manager should be appointed to coordinate

⁶ An FI can adopt the business impact analysis methodology to assist in its identification of critical business services and functions.

incident management across the affected functions, and oversee the resumption of the business service in the event of a disruption.

3 Service Recovery Time Objective

3.1 FIs should establish the **Service Recovery Time Objective (SRTO)** for each critical business service. The SRTO, being a time-based metric, provides clarity between FIs and their third parties on the recovery expectation of the business service. This will help to facilitate decision-making and monitoring of the progress of its recovery following a disruption.

3.2 In establishing SRTOs, FIs should take into consideration its obligations to customers, and the financial ecosystem and its participants. FIs are expected to put in place recovery strategies⁷ to enable them to achieve the established SRTOs and recover to the service levels required to meet their business obligations. For critical business services that are supported by a number of business functions, FIs must ensure that the Recovery Time Objectives (RTOs) of the underlying business functions and their dependencies will meet the SRTOs.

3.3 FIs should also set out clear and defined thresholds for BCP activation in the event where the performance of a critical business service is reduced or intermittent, but not to the extent that it is completely unavailable. This will guide the FI in activating its BCP in a timely manner, before the performance degradation becomes overly prolonged or worsened to the extent that it results in severe impact.

⁷ Examples of recovery strategies could include manual workarounds, activation of alternate sites, and expansion of the service capacity of alternate delivery channel(s) to meet the increase in demand.

4 Mapping of Interdependencies

People, Processes and Technology

4.1 The financial sector has become increasingly interconnected with the growing reliance on common IT systems and third parties. As a first step to mitigate the risks arising from the interdependencies, FIs should identify and map the end-to-end dependencies on people, processes, and technology, including those involving third parties, that support each critical business service.

4.2 The dependency mapping will enable FIs to identify resources critical to the service delivery, consider the implications of their unavailability, and address any gaps that could hinder the effectiveness and safe recovery of the critical business services. FIs should use the information derived from the dependency map to verify that the recovery of the business functions and their dependencies, will meet the established SRTOs.

Third Party Dependencies

4.3 Most FIs engage third parties⁸ to support the delivery of their critical business services. These arrangements could increase operational risks arising from the failure, delay, or compromise of a third party in providing the service.

4.4 The FI should perform its due diligence to obtain assurance that the SRTOs of the critical business service can be met by the third parties. This assurance can be obtained through measures, such as the following, where possible:

- (a) Establish and regularly review operational level or service level agreements with third parties that set out specific and measurable recovery expectations;
- (b) Request for dedicated manpower from their third party service providers for specialist functions that cannot be performed in-house; or
- (c) Conduct audits, regular tests or joint tests with their third parties to ensure that the third parties have the ability to support FIs even in the scenario that these third parties experience disruptions.

⁸ These include third party service providers as well as intra-group service providers.

4.5 FIs should also put in place plans and procedures⁹ to manage and address any unforeseen disruption, failure or termination of third party arrangements to minimise the impact of such adverse events on their business continuity.

4.6 Some interdependency risks (e.g. unavailability of telecommunications networks, power utilities, etc.) may be beyond an FI's direct control to mitigate completely. Hence, it is important that FIs put in place risk mitigating measures, such as implementing redundancy or back-up arrangements, to address the interdependency risks posed by the disruption of these services.

⁹ Examples include pre-designating an alternate service provider or building up in-house capability in the event that the primary service provider is unavailable to provide immediate support.

5 Concentration Risk

5.1 While there are economic benefits to be gained through the centralisation of operations, concentration risk may arise when there is concentration of people, technology or other required resources in the same zone¹⁰. FIs may also be exposed to concentration risk when several of its critical business functions are outsourced to a single provider. As skilled people, information, and systems are important assets that are difficult to replace quickly, FIs will need to adopt a sound and responsive risk management to address concentration risk.

5.2 FIs could consider adopting the following approaches to mitigate concentration risk:

- (a) **Primary-secondary site operation** – Separate primary and secondary sites of critical business services or infrastructure (such as data centres) into different zones to mitigate wide-area disruption;
- (b) **Critical business functions segregation** – Separate critical business functions into different zones to mitigate the risk of losing multiple critical business services from a wide-area disruption;
- (c) **Split team and back-up team arrangements** – Diversify personnel supporting each critical business function across different zones, or establish reserve team arrangements¹¹ for critical business functions to eliminate the dependency on a single labour pool;
- (d) **Cross-training** – Identify critical skills or roles, and develop cross-training programs to build versatility for key personnel involved in these roles;
- (e) **Cross-border support** – Allow cross-border support of critical business functions during disruptions;

¹⁰ A zone refers to an area or region that shares a similar risk profile such that in the event of a disruption, people, information, and systems, located in the same zone would likely to be affected. Due to a number of factors such as the differing size and complexity of business operations across FIs in Singapore, it would not be appropriate nor practical, to standardise on a criteria that defines a zone that could be applied equally across the financial sector.

¹¹ FIs could consider establishing operationally ready reserve team(s) to substitute the team(s) currently performing critical business functions in the event they need to be isolated to curb the spread of an infectious disease. The reserve team(s) could comprise personnel who are not in contact with the original team until being activated to support the critical business functions.

- (f) **Alternative service provider** - Pre-designate an alternate service provider in the event that the primary service provider is unavailable to provide immediate support;

5.3 Taking into consideration learnings from COVID-19, FIs should be cognisant of the resultant risks from the implementation of alternate work arrangements to mitigate the risk of disease transmission at workplaces. Alternative work arrangements may entail changes to policies, operational processes, and use of equipment or IT systems that pose new operational risks and other challenges¹². FIs can consider putting in place mitigating controls¹³ to address such new risks and challenges.

¹² Examples of such new operational risks and challenges could include the capacity, resiliency and security of infrastructure to support remote working arrangements, or the ability to enable cross-border support.

¹³ Examples of mitigating controls include establishing alternative locations to allow personnel to resolve hardware issues or automating processes to reduce dependencies on critical personnel.

6 Continuous Review and Improvement

6.1 While globalisation and technological advancement bring about opportunities for FIs to improve their business processes, the reliance on technology and third parties also poses greater risk exposure to FIs. FIs should proactively address such risks, and continuously seek out areas to enhance and ensure that their BCM remain relevant and forward looking. This will strengthen FIs' abilities to manage any unforeseen disruption to their business services.

Threat Monitoring, Review and Reporting

6.2 FIs should actively monitor and identify external threats and developments that could disrupt the normal operation of their business services, and have an escalation process to alert internal stakeholders and senior management about the relevant threats in a timely manner.

6.3 FIs should institute processes to conduct environmental scanning for relevant risk events, such as natural disasters, terrorism, pandemic outbreaks, and cyber incidents. FIs should also monitor the public advisories issued by relevant authorities to obtain the latest information and guidance on emerging threats that may pose a risk to their business continuity.

On-going Improvement

6.4 An FI should review its BCM policies, plans, and playbooks to identify areas of improvement and address any gaps in its processes following an operational disruption. An FI should also draw lessons learnt from its own near misses, as well as incidents in other organisations, to enhance its business continuity preparedness.

6.5 An FI should regularly assess the need for additional tools and automation to enable it to manage an incident or disruption more effectively. These could include implementing tools¹⁴ that enhance the FI's BCM implementation or crisis management to better facilitate decision-making during a disruption.

6.6 An FI should update and evolve its BCM policies, plans, and playbooks based on changes in its operational environment and the threat landscape. An FI should review its

¹⁴ These tools could include automated workflows, templates and checklists, communications tool for activation and notification of personnel, situational dashboards providing real-time updates on the incident etc.

critical business services, their respective SRTOs, and dependencies at least annually, or whenever there are material changes to the people, process or technology involved in maintaining the smooth and continued delivery of critical business services.

7 Testing

7.1 Testing is crucial in validating an FI's BCM preparedness. FIs should conduct regular and comprehensive testing to gain assurance that their response and recovery arrangements are robust, and enable them to continue the delivery of critical business services in a timely and reliable manner following a disruption.

7.2 FIs should plan their test activities to meaningfully test all aspects of their BCM frameworks, and to meet the following objectives:

- (a) Validate and measure the effectiveness of the BCPs using appropriate metrics, and remediate any gaps or weaknesses that are identified in the recovery process;
- (b) Familiarise personnel involved in business continuity and crisis management with their roles and responsibilities, including how the alternate sites and recovery arrangements should be operated, so as to improve coordination and ensure a seamless execution of plans;
- (c) Sensitise senior management involved in crisis management (and their alternates) to the potential areas of concern that could arise in crisis situations, and practise making decisions under simulated conditions, including scenarios that require prioritising the recovery of competing critical business services;
- (d) Stress test BCPs under severe but plausible scenarios to allow FIs to challenge their current planning assumptions and ensure the relevance and effectiveness of their BCPs, to better mitigate the impact of severe disruptions; and
- (e) Verify that the SRTOs of its critical business services can be met through the established recovery strategies.

7.3 FIs should select the types of tests¹⁵ that best meet these objectives, and set out the frequency and scope¹⁶ of these tests to commensurate with the criticality of the business services. An FI should also properly document all its test records, clearly indicating details, such as the test objectives, scope, scenario design, participants involved, results and follow-ups for each test.

Remedial actions

7.4 Being able to clearly track and assign ownership of remedial actions are essential in ensuring that lessons learnt are systematically captured and used to improve the existing recovery processes. FIs should establish a formal process to follow up on the remedial actions identified in each test. The effectiveness of the remediation measures undertaken should also be validated at subsequent tests to ensure proper implementation.

Industry exercises

7.5 FIs are strongly encouraged to participate in industry and cross-sector exercises¹⁷ organised by government agencies, regulatory bodies, industry associations, and financial market infrastructure operators. Doing so would strengthen the joint responses and coordination between institutions and improve confidence in the financial sector's overall business continuity capability.

7.6 These exercises provide opportunities for the participating institutions to consider and discuss the impact of their individual actions on their counterparties in light of the external interdependencies they may have on each other. This will allow FIs to gain valuable insights to improve their BCM policies, plans and playbooks.

¹⁵ Types of test could range from basic call-tree activation and component failover of specific applications, to more complex and integrated exercises covering failovers, restoring data from back-up media, alternate data centre or alternate site activation, business process recovery tests, operating with reduced headcount, operating in the absence of a key third party, relying on onsite generators for a prolonged period etc.

¹⁶ Scope of the tests would involve scenario design to determine the components to be tested (e.g. incident management, crisis management, crisis communications, recovery of critical business services, alternate site activation and operation, retrieval of vital records, unavailability of critical staff or key third parties, and familiarity with the tools and automation), as well as the involvement of participants.

¹⁷ Examples of such exercises include business continuity exercises organised by the Association of Banks in Singapore, contingency tests organised by the Singapore Automated Clearing House, MEPS+ contingency exercises organised by the Monetary Authority of Singapore, and business continuity tests by the Singapore Exchange.

8 Audit

8.1 A BCM audit is an important means to provide the FI with an independent assessment on the adequacy and effectiveness of the implementation of its BCM framework. An FI should ensure that its audit programme adequately covers the assessment of BCM preparedness based on the level of operational risks that it is exposed to.

8.2 The scope and frequency of BCM audits¹⁸ should be commensurate with the criticality of the business services and business functions. The BCM audits should be conducted by a qualified independent party (e.g. qualified internal or external auditor).

8.3 The FI should establish processes to track and monitor the implementation of remedial actions in response to the audit findings. FIs should escalate any significant audit findings on lapses that may have severe impact on the FI's BCM to the Board and senior management. The FI should submit the BCM audit reports to MAS upon request.

¹⁸ Examples of BCM audits include institutional-wide BCM audits, specific service or function-level audits covering BCM preparedness, or thematic audits.

9 Crisis Management and Communications

9.1 The senior management is responsible for steering the FI out of a crisis by overseeing its crisis management activities. To aid the senior management in responding to a crisis, the FI should have in place:

- (a) A crisis management structure, with clearly defined roles, responsibilities, reporting lines, and chain of command (including designating alternates to primary representatives);
- (b) A set of pre-defined triggers and criteria for timely activation of the crisis management structure;
- (c) Plans and playbooks to guide the FI on the course of actions and decisions to be made during a crisis;
- (d) Tools and processes to facilitate timely updating and assessment of the latest situation to support decision-making during a crisis;
- (e) A list of all internal and external stakeholders to be informed when a critical business service is disrupted, and communications requirements (e.g. notification criteria, notification timelines, update frequency etc.) for each stakeholder; and
- (f) Communication channels (including mainstream and social media) to effectively communicate with its stakeholders, including alternative channels that can be used when the primary communication channel is unavailable.

Communications with Staff

9.2 The FI should have in place channels to update staff on developments during a crisis. This include cascading timely information that staff should take note to protect their safety, as well as sending out messages on staff welfare to manage staff morale. The FI should also ensure that staff who experience psychological trauma from a crisis has access to crisis counselling support.

Communications with External Stakeholders

9.3 The FI should ensure that communications to its external stakeholders (e.g. customers, media, government authorities and regulators, etc.) are proactive, transparent,

and factual. This will reassure stakeholders and maintain customer confidence during a disruption or crisis.

9.4 To facilitate timely public communications during a crisis, the FI should prepare drawer media statements that cater to different scenarios, and holding statements that can be released immediately in the event of a disruption. FIs should also coordinate with peer FIs through the relevant industry associations to achieve consistent messaging to the public in the event of a widespread disruption. The FI should also identify its designated spokespersons who will be responsible to address the media and the public during a crisis.

9.5 FIs should ensure that MAS is notified immediately¹⁹ of incidents where business operations are, or will, be severely disrupted, or when the BCP is activated, or going to be activated in response to an incident. In the notification, the FI should provide information, such as the assessed impact to its customers and the actions that have been taken (e.g. activation of alternative service channels, alternate sites or manual procedures, public communications, etc.).

¹⁹ FIs should notify the Authority through their review officers or the MAS BCM Hotline.

10 Responsibilities of Board and Senior Management

Oversight and Governance

10.1 The Board and senior management are ultimately responsible for the FI's business continuity. A prolonged disruption in the performance of the FI's critical business services could significantly impair its reputation, financial safety and soundness, or in some instances, the proper functioning of the financial ecosystem.

10.2 The Board and senior management should therefore provide leadership, strategic direction, and establish strong governance over the FI's BCM. This would ensure that the FI has the ability to effectively respond to, and recover from a wide range of operational disruptions.

10.3 The Board²⁰ and senior management should build an organisational culture that has business continuity preparedness embedded within the FI's day-to-day risk management²¹, and integrated within the FI's operational risk management framework to enable effective identification and management of the risks across the organisation.

10.4 The Board, or the committee delegated by it, should be responsible to ensure that:

- (a) An effective and comprehensive BCM framework is established and maintained to manage potential operational disruptions;
- (b) A BCM function or equivalent is established and sufficiently resourced to oversee the organisation-wide implementation of the BCM framework to achieve the desired state of business continuity preparedness;
- (c) The senior management, who is responsible for executing the FI's BCM framework, has sufficient authority, competency, resources, and access to the Board;

²⁰ The Board may delegate the authority to make decisions to a Board committee but bears the ultimate responsibility. Please refer to MAS Guidelines on Risk Management Practices – Board and Senior management. For FIs headquartered outside Singapore, the responsibility of the Board may be delegated to a management committee or body responsible for the supervision and oversight for the FI's operations in Singapore.

²¹ As an example, the FI's change management process for businesses and systems should consider if the proposed change could have implications to the FI's business continuity preparedness, and if corresponding changes to the BCPs are necessary.

- (d) The established SRTOs of the respective critical business services are commensurate with its business needs and obligations;
- (e) The effectiveness of the BCM framework is regularly reviewed and evaluated against external events, changes in risk profiles and business priorities, or new processes, systems, or products or services; and
- (f) An independent audit is performed to assess the effectiveness of controls, risk management and governance of business continuity preparedness of the FI.

10.5 The senior management should ensure that:

- (a) The BCM framework is established to support and manage the development, implementation, and maintenance of effective BCPs and measures, taking into consideration recovery arrangements by third parties;
- (b) Sound and prudent policies, standards and procedures for managing operational disruptions are established and maintained, and standards and procedures are implemented effectively;
- (c) Roles and responsibilities for maintaining the FI's business continuity preparedness are established and defined clearly;
- (d) Measurable goals and metrics are used to assess the FI's overall business continuity preparedness;
- (e) Business services and functions that are critical to the FI are identified, and their recovery time objectives are established;
- (f) The crisis management and communications structure, and BCPs are tested on a regular basis to validate their effectiveness against severe but plausible operational disruption scenarios and verify that the critical business services are able to recover within their SRTOs;
- (g) Gaps and weaknesses identified from the FI's business continuity testing, post-mortems of incidents, audit, or other risk management programmes (e.g. risk and control self-assessments, etc.) are remediated in a timely manner; and
- (h) A training programme is established and reviewed annually to ensure that all staff who have a role in the FI's BCM are familiar with their roles and responsibilities.

10.6 The senior management should provide an annual attestation to the Board on the state of the FI's BCM preparedness, the extent of its alignment with the Guidelines, and key issues requiring Board's attention such as significant residual risk and assessment of BCM readiness. The attestation should also be provided upon MAS' request.

Appendix: Examples of Business Services

Types of Business Services	Examples of Business Services ²²
Banking	Cash transactions Lending Deposit-taking Treasury Private banking and wealth management Investment banking or corporate finance Trade services
Insurance	Claims servicing (including surrender) Policy renewal and servicing Policy inception
Financial Market infrastructures	Derivatives trading, clearing, settlement and reporting Securities trading, clearing, settlement and depository Administering of benchmarks Payments clearing and settlement
Broking and Custody	Trading, clearing, settlement and custody
Asset Management	Portfolio management and trading Trade settlement and operations Trustee services, including fund admin and valuation Processing of subscriptions and redemptions in fund units (transfer agency)
Payment Services	Cross-border and domestic funds transfer Credit/debit card payments E-wallet payments/ prepaid card payments

²² These examples listed are non-exhaustive. FIs should identify the business services that are critical depending on the nature, size, and complexity of its business operations.

5 ANNEX C – Response to Feedback Received from First Consultation Paper

Critical Business Functions and Business Continuity Objectives

Business Service

5.1 Respondents supported MAS' approach for FIs to implement Business Continuity Management (BCM) policies, plans and playbooks at the service level. This would allow FIs to identify the complete set of processes supporting the service, draw out any internal or external dependencies that could have an impact on the delivery of the service, and identify potential gaps. This is opposed to taking a silo approach of implementing BCM only at the business unit or department level, where the focus would be on the recovery of individual processes.

5.2 However, respondents highlighted that business functions are commonly referred to as business processes performed by individual organisational lines (i.e. department or unit), and the change in taxonomy to refer business function as a service that an FI provides to its customers, could lead to interpretation issues in the implementation of BCM within the FIs' operations. Respondents also sought clarification on the definition of customer, and whether the scope includes internal customers or stakeholders within the FIs.

MAS' Response

5.3 MAS' original intent was to align the definition of "business function" with the definition of "critical functions" in MAS Notice 654 Recovery and Resolution Planning (RRP). MAS acknowledges the respondents' feedback, while also recognising the differences in objectives and scope between the RRP Notice²³ and the Guidelines. In that regard, MAS agrees with respondents to retain the definition of "business function" as processes performed by business units in the FI. We have hence introduced a new term "business service" into the Guidelines for added clarity and to avoid unnecessary changes to the FI's current BCM framework. The remainder of this consultation response paper will henceforth refer to "business service" as a service that an FI provides to its external customers, and refer to "business function" as activities or processes performed by business units in the FI.

²³ For the purpose of RRP, FIs should continue to refer to the definitions in MAS Notice 654.

Therefore, both this response paper and the second consultation paper will adopt the ordinary meaning of “customer”.

Critical Business Services and Functions

5.4 Respondents requested for further guidance on the identification of critical business services based on the potential financial and non-financial loss when these services are disrupted. Guidance was also sought on whether services should be differentiated according to product types or business lines.

5.5 Respondents opined that critical or time-sensitive business functions that do not support any business service but are necessary to support the proper functioning of the FI during a disruption should also be recovered. Examples of such functions cited were IT support and human resource, etc.

MAS' Response

5.6 FIs are best placed to identify their critical business services based on the impact of the service disruption on the FI's safety and soundness, customers as well as on other participants in the financial ecosystem. We have included some of these considerations in the revised Guidelines. Likewise, MAS will not prescribe whether services should be differentiated by product types or business lines in view of the differing size and complexity of business operations across the FIs.

5.7 MAS agrees that functions that are not directly supporting a business service but are critical in supporting the FI during a disruption – such as maintaining the FI's safety and soundness – should also be prioritised for recovery. Therefore, we have included in the revised Guidelines that MAS expects FIs to have the necessary recovery strategies in place for these critical business functions to maintain public confidence in the FI, mitigate the impact of service disruption to its customers and to prevent any contagion effects on the financial system.

Recovery of critical business services

5.8 Respondents sought clarification on whether the level of output defined in the minimum performance level (“MPL”)²⁴ refers to processing capacity. It was highlighted that MPL may not be applicable or meaningful for some services and it is challenging for an FI to consider all circumstances such as market condition, risk appetite, nature of incident to pre-determine the MPL. Respondents also raised concerns that the MPL is too broad to quantify as it may not be a summation of the recovery time objectives (“RTO”) of the processes within the business service when processes are not executed sequentially.

MAS’ Response

5.9 MAS agrees that the MPL could be difficult to quantify for certain type of services. Rather than setting the MPL as a recovery target, MAS has introduced “Service Recovery Time Objective (SRTO)” as a new term, in lieu of MPL, in the second consultation paper. SRTO refers to the target time to recover a critical business service to a level sufficient to meet its business obligations, or the acceptable duration before the disruption of a critical business service would result in severe business impact and losses to the FI and any of its customers. The use of SRTO, which is a time-based metric, provides clarity between the FI and their third parties, on the recovery expectation during a disruption.

5.10 In establishing the SRTO, FIs should take into consideration its obligations to the customers, financial ecosystem and its participants. During a disruption, FIs are expected to meet the SRTO through measures, such as manual workarounds, activation of alternate sites, or expansion of the service capacity of alternate delivery channel(s) to meet the increase in demand. For critical business services that are supported by a number of business functions, FIs should ensure that the RTOs of the underlying business functions and their dependencies will meet its SRTO.

Incorporating third parties’ processes and capabilities into recovery planning

5.11 Respondents highlighted that FIs may not be able to obtain sensitive or confidential information from third parties²⁵, such as information relating to their business processes and recovery capabilities, to be incorporated into the “end-to-end” recovery planning. For

²⁴ MPL is defined in the 2019 consultation paper as the minimum level of output that an FI will aim to recover to in its initial phase of recovery following a business disruption.

²⁵These include third party service providers as well as intra-group service providers.

example, a securities broker's business processes would involve third parties, such as the exchange, clearing house or depository.

5.12 Respondents also highlighted that it will be onerous for FIs to account for the recovery capabilities of third parties and requested for flexibility on the approach to address the residual risks posed by these interdependencies. They further expressed concerns that common service providers, such as telecommunications and utilities (water, electricity etc.) providers, financial rating providers and payment networks providers may not agree to disclose their recovery time objectives or conduct joint tests.

MAS' Response

5.13 MAS expects FIs to obtain assurance from relevant third parties that they are able to support the delivery of the critical business service within its SRTO. The assurance can be obtained through measures such as establishing operational level or service level agreements, requesting for dedicated people from their service provider, and conducting audits, regular tests or joint tests with their third parties. The RTOs of third party services that are key to the recovery of critical business services should also be captured in the "end-to-end" dependency mapping²⁶.

5.14 The FI's senior management remains ultimately responsible for the continuity of the critical business services. In view of the increased reliance on third party service providers, MAS expects FIs to take reasonable measures to minimize the impact of disruption to services provided by third parties. These measures could include putting in place risk mitigating measures, such as implementing redundancy or back-up arrangements (e.g. alternate service provider, alternate delivery channels, alternate sites or manual processes, plans and procedures) to manage and address any unforeseen disruption, failure and termination of third party arrangements.

Accountability for a Service

5.15 Respondents highlighted that it will be challenging to assign ownership, accountability, and responsibility for the delivery of a service, that is typically owned by a number of business units across the organisation.

²⁶ Dependency mapping is defined as a process to identify and understand the internal and external dependencies on people, processes, and technology, including those involving third parties, that support each critical business service.

MAS' Response

5.16 The FI's senior management is ultimately responsible for ensuring the continuity of the critical business services. In instances whereby a critical business service is supported by more than one business unit, it is even more critical that all relevant business units be involved in determining the SRTO, and in identifying and remediating any potential gaps in its recovery process through dependency mapping.

Intermittent service availability

5.17 Respondents highlighted that reduced or intermittent service availabilities are usually managed through day-to-day incident management or the activation of IT disaster recovery to fully recover a system, and may not necessitate the activation of business continuity plans (BCPs). They suggested that the establishment of monitoring capabilities for prompt detection of reduced or intermittent service availabilities should be addressed under the Technology Risk Management Guidelines instead, since these are largely attributed to the intermittent availability of systems.

MAS' Response

5.18 The establishment of monitoring capabilities for prompt detection of reduced or intermittent services due to system issues has been included in the Technology Risk Management Guidelines²⁷. Nevertheless, an FI may be required to activate its BCP in a timely manner, before the performance degradation becomes overly prolonged or worsens to the extent that it results in severe impact. In this regard, MAS expects FIs to set out clear and defined thresholds for BCP activation in the event where the performance of a critical business service is reduced or intermittent, but not to the extent that it is completely unavailable. This is based on lessons learnt from previous incidents, where FIs were not able to address the issue of intermittent or degraded services through their remediation measures, and did not activate their BCPs in a timely manner, resulting in prolonged service unavailability.

²⁷ The FI should continuously monitor the utilisation of its system resources against a set of pre-defined thresholds. Such monitoring could facilitate the FI in carrying out capacity management to ensure that IT resources are adequate to meet current and future business needs.

- *Technology Risk Management Guidelines, January 2021, 8.1 System Availability*

Responsibility of the Board and Senior Management

Oversight by the Board

5.19 MAS had proposed in the 2019 Consultation Paper (Paragraphs 4.3(b) and 4.3(c)) that the Board of directors (“Board”)²⁸ be responsible for reviewing and endorsing the FI’s critical business functions, business continuity objectives, and the adequacy of resources. Respondents highlighted that the Board should provide strategic directions instead of managing day-to-day running that includes approving critical business functions, business continuity objectives, budgets, and staff allocation responsibilities.

5.20 Some respondents sought clarification on the appropriateness of a management committee to assume the responsibility of the Board, for an entity incorporated outside Singapore or for a small entity that may have a very lean organisation structure.

MAS’ Response

5.21 MAS agrees that the operational responsibilities that are under the purview of the senior management should be not duplicated at the Board. Instead, the Board should provide oversight by ensuring that the senior management has allocated adequate budget and resources to implement effective business continuity measures to achieve the desired state of preparedness, that commensurate with its business needs and obligations. The responsibility of the Board has been clarified in the revised Guidelines.

5.22 For FIs headquartered outside Singapore, the responsibility of the Board may be delegated to a management committee or body responsible for the supervision and oversight for the FI’s operations in Singapore. For smaller FIs, the responsibility of the Board can be assumed by the local senior management provided that the responsibilities of Board can be effectively discharged.

²⁸ “Board” refers to:

(i) in the case of an FI incorporated in Singapore, the Board of directors; and

(ii) in the case of an FI incorporated or established outside Singapore, a governing body or committee beyond local management that is charged with oversight and supervision responsibilities for the FI’s operations in Singapore.

- Guidelines on Individual Accountability and Conduct

Responsibility of Senior Management and Committee to oversee BCM

5.23 Several respondents sought clarification on whether the committee to oversee the FI's BCM is responsible for the implementation of BCM in the FI, or if the committee is responsible for reviewing the FI's BCM framework. This will allow them to assess the appropriateness of appointing the Chief Risk Officer or a member of senior management to lead the committee as well as to determine the composition of the committee. They highlighted that business heads are responsible for the recovery of an FI's business operations during a disruption and suggested that there should be a clear segregation between risk ownership and the risk review function.

MAS' Response

5.24 BCM is part of the FI's overall risk management to manage the risks arising from disruptive events. As the responsibilities of the Chief Risk Officer relate to the identification, monitoring, and management of the risks of the FI, it is appropriate for the Chief Risk Officer to also have purview over risks related to BCM. At the same time, FIs are given discretion to decide on the structure that best facilitates the implementation and the management of their BCM. The Guidelines have been amended to focus on the responsibility of the senior management on the FI's BCM that includes putting in place a programme for the development, implementation and maintenance of BCPs, the assessment of the overall business continuity preparedness, and addressing gaps and weaknesses identified.

Support from Group or Regional Office on implementation of BCM

5.25 A few respondents sought clarification on whether FIs can continue to rely on support provided by the Group or Regional Office, such as to leverage Group or Regional policies to comply with the Guidelines, or have senior management based overseas be responsible for the FI's BCM. They opined that there is a risk of potentially less effective BCM and duplicative efforts if they were to implement a segmented or localised approach for BCM.

MAS' Response

5.26 FIs may adopt and adapt the BCM frameworks, policies, and procedures that have been instituted at the Group or Regional level, as long as these arrangements would enable the FIs' Singapore operations to comply with the Guidelines. MAS agrees that senior management, who are based overseas and are responsible for the implementation of BCM in the Singapore's operations, can continue to be responsible for the BCM implementation of the FI in Singapore under a regional or global management arrangement.

Crisis Management Team, Crisis Activities and Training

5.27 Respondents provided feedback that the composition of the Crisis Management Team (CMT) may not comprise of entirely of senior management, and it could differ from FI to FI depending on the FI's size of operations, or alignment with the regional or global organisation structure. For example, FIs of smaller size may form their CMTs comprising of senior management and other staff, while FIs with regional or global operations may adopt a regional or global Crisis Management setup with representatives based overseas.

5.28 Respondents also highlighted it may not be practical to prescribe parameters for decision-making such as setting (a) a maximum time allocated to assess and activate the recovery arrangements and (b) a potential work routine during prolonged outage. Instead, they recommended that an FI's CMT should be allowed to assess and decide on the activation or the arrangements depending on the circumstances and severity of the crisis.

5.29 Respondents also sought clarification on the expectations of training the CMT members on an annual basis, especially in view of the limited crisis management courses or training available.

MAS' Response

5.30 MAS agrees that FIs should determine the composition of the CMT that is appropriate to their size and organisation structure. FIs are expected to set out a crisis management structure with clearly defined roles, responsibilities, and chain of command (including designating alternates to primary representatives).

5.31 MAS agrees that FI's CMT should assess and decide on the course of action to be undertaken based on the circumstances and severity of the crisis. However, FIs should identify a set of pre-defined triggers and criteria to facilitate timely activation of the crisis management structure for decision-making. The Guidelines have been amended to reflect an outcome driven approach to crisis management.

5.32 The senior management is responsible for steering the FI out of a crisis. FIs should accord proper training to their senior management to familiarise them with the crisis management structure and their responsibilities during a crisis. Hence, the Guidelines have been revised to provide FIs with the flexibility to implement training in the format assessed to be most effective in achieving this outcome.

Business Continuity Plans

Business Continuity Plans (BCPs) for Critical Business Services

5.33 Respondents sought clarification on the expectations to document supporting functions in each service's BCP as well as to include the list of non-exhaustive components in the BCP as set out in the 2019 Consultation Paper Paragraph 5.16. They suggested for MAS to allow FIs to provide the end-to-end perspective for service by referencing or mapping the dependencies of the underlying processes while ensuring recovery processes are aligned in the respective unit level BCPs. This approach will avoid an overly complex BCP which could lead to duplication between services' BCPs that have the same functions supporting.

5.34 A few respondents also highlighted that certain processes are automated and may not have manual workaround or alternatives. They sought guidance on the treatment for such automated processes.

MAS' Response

5.35 The objective of documenting end-to-end interdependencies is to ensure that FIs consider all the functions and dependencies supporting a critical business service to meet the SRTO. FIs should document the dependencies on people, processes, technology and other resources, including those involving third parties, that support each critical business service in a structure most suitable for its business operations. The dependency map can be established in addition to the existing business unit or business function-level BCPs.

5.36 In the event that a critical business service relies on automated processes that have no manual workarounds, the FI must be able to recover the automated processes quickly or put in place appropriate contingency measures (e.g. alternative systems or expansion of the service capacity of alternative delivery channels) in order to meet the SRTO when any of those automated processes is disrupted.

Risk assessment and Plausible Scenarios

5.37 Respondents sought clarification on whether the expectation is for FIs to conduct a risk assessment for each service, or whether the same risk assessment process could be applied at the organisational level, since a number of services would be affected by the same threat scenario.

5.38 Respondents queried if the expectation is for FIs to provide an exhaustive list of plausible scenarios in their BCPs. They provided feedback that it would be impractical for FIs to incorporate all plausible scenarios in their BCPs, and suggested that the BCPs should focus on recovery processes and resources based on the type of disruption, such as loss of physical infrastructure, etc.

MAS' Response

5.39 MAS expects an FI to identify severe but plausible scenarios and stress test the effectiveness of their BCPs against these scenarios. The identification of the scenarios can be conducted from an organisation-wide perspective and/or at the individual service level depending on their business set-up, so long as it can provide the necessary planning scenarios and assumptions to form the basis of their recovery strategies and plans.

5.40 While MAS agrees that FIs should plan their BCPs around the type of disruption, FIs should also cover scenarios, where the disruption could have a simultaneous impact on the availability of people, IT systems, supply chains or physical facilities.

Formal BCM training programme

5.41 Respondents provided feedback that tests are effective ways to ensure staff's familiarity with BCP processes, but sought clarification on whether tests could also qualify as formal training for staff with BCM responsibilities, including functions outsourced to third party.

MAS' Response

5.42 BCM tests and drills are not substitutes for BCM training. The objective of BCM training is to ensure that staff are able to execute their BCM roles and responsibilities effectively, particularly for staff whose business-as-usual roles are not directly related to their responsibilities under BCM (e.g. crisis communications, corporate first responders etc.). FIs can determine the type and format of training activities that are needed to achieve this outcome.

Incident notification to MAS

5.43 Respondents sought clarification on the definition of incident or criteria for notifying MAS of an incident to critical business service, especially if there is no impact to customers. They also seek to understand if the existing incident notification template can be used.

MAS' Response

5.44 FIs should inform MAS immediately of incidents where business operations are, or will be severely disrupted, or when the business continuity plan is activated, or going to be activated in response to an incident. FIs should continue to update MAS of such incidents per the [MAS incident reporting template](#).

BCM Tests

Scope, type, and frequency of BCM tests

5.45 Respondents sought clarification on the expectation to validate all aspects of a service's BCP and crisis management plan, as well as the conduct of annual BCP test for each critical service. Respondents asked if there is an expectation to conduct different types of complex tests for each critical service and function. There were concerns on conducting "end-to-end" testing of services, which could translate to increased operational risks due to the interlinkages between systems.

5.46 Respondents also gave feedback that different types of tests may achieve the same objective and conducting such extensive testing will result in testing fatigue due to multiple tests of same functions supporting the different services. They suggested MAS to allow FIs to determine the scope, type and frequency of BCM tests that commensurate with the scale, nature and complexity of the FIs' operations.

MAS' Response

5.47 MAS agrees that the types and frequency of tests should commensurate with the criticality of the services and functions. To ensure BCM preparedness, FIs should conduct regular and comprehensive tests by clearly setting out their test objectives and scope. These objectives should include validating that their crisis management and communications structure, and response and recovery arrangements are effective against severe but plausible operational disruption scenarios. With these in mind, FIs should develop a testing programme to meet these expectations. The Guidelines have been amended to clarify the expectations on testing.

Involvement of third parties

5.48 Respondents also highlighted the challenges of involving third parties in “end-to-end” testing of a service and sought clarification on alternative means to obtain assurance on third parties’ recovery capabilities. It was highlighted that individual FIs have limited control over the testing of third parties such as financial market infrastructures, utilities providers, and cloud service providers, and it is impractical to conduct joint testing given the number of FIs these third parties support.

MAS’ Response

5.49 MAS acknowledges the concerns in relation to testing with third party service providers (e.g. financial utility providers). Under circumstances where joint testing with third party service providers is not possible, MAS expects the FIs to obtain assurance from relevant third party service providers through measures such as reviewing the results of tests conducted by service providers.

Involvement of all CMT members in a test

5.50 Respondents sought clarification on the expectation to involve all primary and alternate CMT members in a crisis management test on an annual basis. They raised challenges in coordinating and scheduling a test involving all CMT members (inclusive of both primary and alternates) and suggested that their involvement can be decided based on the type and objective of test.

MAS’ Response

5.51 MAS agrees that FIs should have the discretion of deciding the involvement of CMT members based on the test scenario. The objective of the crisis management test is to familiarise personnel involved in crisis management with the crisis management process, and have the CMT members (and their alternates) practise making decisions under simulated conditions, such as prioritising the recovery of competing critical business services.

BCM Audits

Scope and Frequency of BCM audit

5.52 Respondents sought clarification on the need to have a BCM-specific audit process and plan, comprising auditable areas for the coming year and to be approved by the Audit Committee separately. They highlighted that audits on BCM are often performed as part of the business process audits rather than a BCM-specific audit.

5.53 Respondents also sought clarification on the expectations of a comprehensive audit scope, the appropriate frequency based on criticality, and the extent of audit independence. They suggested that the audit frequency and plan should be based on their internal risk assessment or risk-based audit policy and plan such as areas with higher risk ratings should be audited more frequently.

MAS' Response

5.54 The objective of audit is to provide an independent assessment of the adequacy and effectiveness of the implementation of the FI's BCM framework to the FI. MAS agrees that FIs can leverage their internal audit plan, audit methodology and audit cycle to determine the scope and frequency of BCM audit. The BCM audit should be conducted by an independent party (e.g. qualified internal auditor or qualified external auditor). The Guidelines have been amended accordingly.

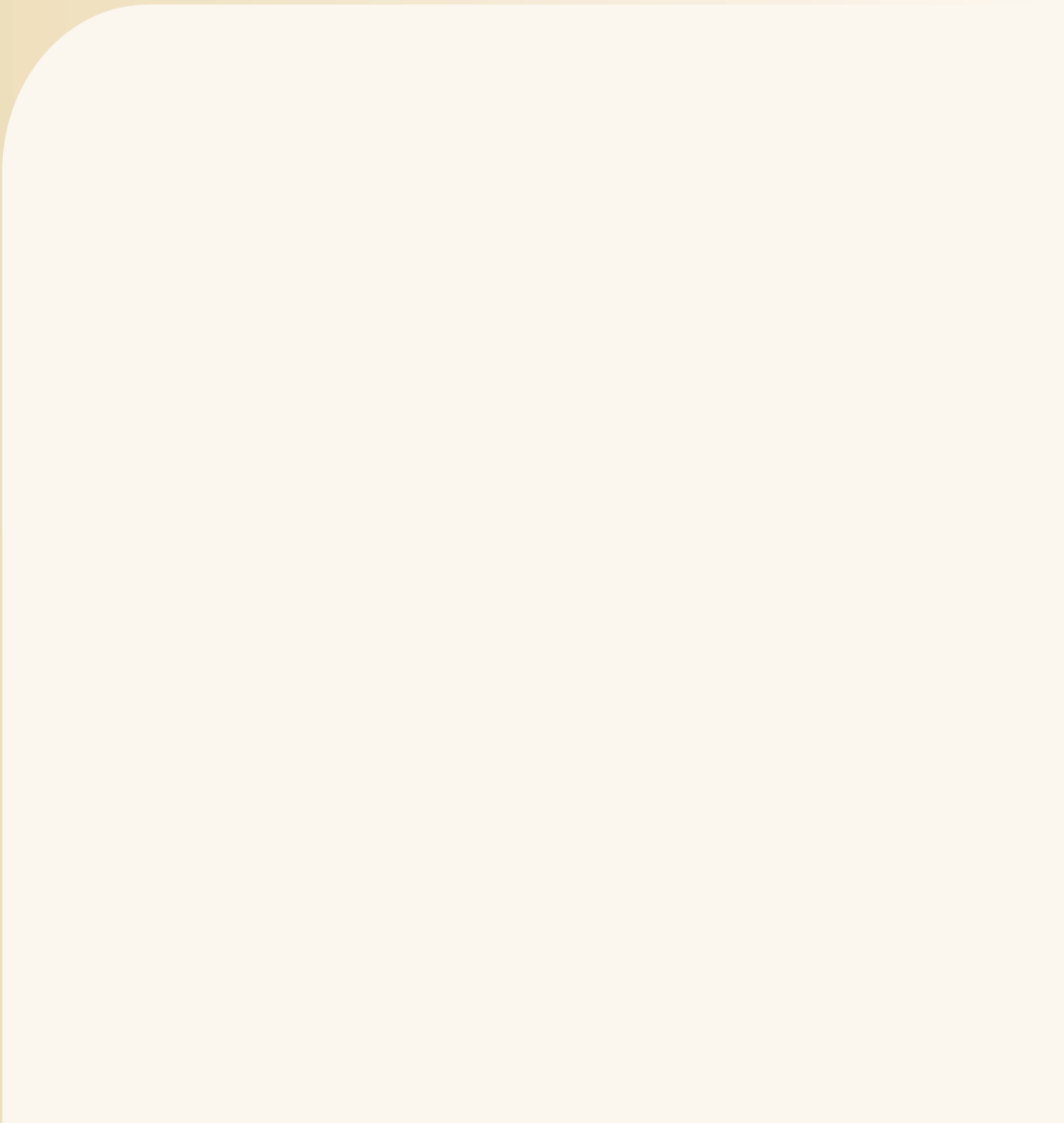
Timeframe for Implementation

5.55 Respondents provided feedback that the implementation of new expectations in the Guidelines would entail changes in their BCM programs and significant efforts. As such, they highlighted that a 12-month transition period would be insufficient and larger FIs may need more time to complete the transition due to the complexity of their operations. They requested for a longer transition timeframe for more complex operations.

5.56 Respondents also sought clarification on the commencement of the audit on BCM and suggested that the audit on BCM should take place a year after transition period.

MAS' Response

5.57 MAS has revised the BCM Guidelines to take in respondents' feedback and is conducting a second consultation. FIs should review the new guidance and provide feedback on the adequacy of 12-month transition period.



Monetary Authority of Singapore