RESPONSE TO FEEDBACK RECEIVED

JUNE 2022

Second Consultation - Proposed Revisions to Guidelines on Business Continuity Management

Monetary Authority of Singapore

Contents

1 Preface

1.1 On 15 October 2021, the Monetary Authority of Singapore (MAS) issued a Second Consultation Paper on Proposed Revisions to Guidelines on Business Continuity Management (BCM) (hereafter referred as "the Guidelines"). The public consultation closed on 15 November 2021.

1.2 MAS would like to thank all respondents for their feedback and comments. MAS' responses to the feedback and comments are set out in the subsequent paragraphs. Unless specifically requested for confidentiality, the respondents' identities and their submissions are provided in Annex A and Annex B respectively.

2 Applicability of the Guidelines

Applicability for small financial institutions (FIs)

2.1 Respondents sought guidance on the applicability of the Guidelines for small FIs, and requested exemption in areas, such as identifying critical business services and performing dependency mapping.

MAS' Response

2.2 As set out in Section 1 of the Guidelines under "Application of Guidelines", the extent and degree to which an FI implements the Guidelines should be commensurate with the nature, size, risk profile 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.

Scope of guidelines and applicability to critical business functions

2.3 Respondents highlighted that while FIs are to identify both their critical business services and functions (as set out in Section 2 of the Guidelines), the subsequent sections of the Guidelines seemed to apply only to critical business services. They sought clarification on whether the Guidelines also applied to *critical business functions.*

2.4 Another respondent asked if it was possible for FIs to have critical business functions that do not directly support a critical business service.

MAS' Response

2.5 The expectations in the Guidelines generally apply to *both* critical business services and functions. However, the expectations to establish the Service Recovery Time Objective (SRTO) and perform dependency mapping are specific to critical business services. The Guidelines have been edited to clearly reflect these.

2.6 Critical business functions can include functions that are not directly supporting any critical business service, but may still impact FIs significantly when they are disrupted. Examples of such functions may include payroll processing, security operations centre, legal and compliance.

Effective Date of the Guidelines

2.7 Respondents provided feedback that the new expectations in the Guidelines would entail changes in their BCM frameworks that require significant time and effort to implement. As such, respondents requested MAS to consider making the Guidelines effective 18 to 24 months after its issuance.

MAS' Response

2.8 MAS recognises that the new concepts introduced in the Guidelines, such as the SRTO and dependency mapping, would require time to implement. At the same time, MAS has also tried to incorporate as much of FIs' feedback from the two consultations as we could. Based on the latest version of the revisions, we are of the view that it is reasonable to expect FIs to meet the Guidelines within 12 months following its issuance. FIs should establish their BCM audit plan within 12 months, and the first BCM audit should be conducted within 24 months of the issuance of the Guidelines.

3 Critical Business Services and Functions

Definition and Applicability of Terms

3.1 Respondents sought clarification on the definition of "critical business service" used in the Guidelines vis-à-vis "critical functions" used in MAS Notice 654 on Recovery and Resolution Planning ("MAS Notice 654"), as well as in both the Financial Stability Board's Recovery and Resolution Planning for Systemically Important Financial Institutions ("FSB Guidance") and the Basel Committee on Banking Supervision's Principles for Operational Resilience ("BCBS Principles").

MAS' Response

3.2 The definitions of "critical business service" and "critical functions" are set out in the following documents:

- "Critical business service" in the Guidelines is defined as an external-facing service that is provided to customers of an FI. A disruption of a critical business service is likely to have a significant impact on the FI's safety and soundness, its customers or other FIs that depend on the business service.

- "Critical function" in MAS Notice 654 is defined as activities performed by a bank for third parties where failure would lead to the disruption of services that are vital for the functioning of Singapore's economy and for financial stability due to the bank's size or market share, external and internal interconnectedness, complexity, and cross-border activities.

- "Critical function" in FSB Guidance is defined as activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external and internal interconnectedness, complexity, and cross-border activities.

- "Critical function" in the BCBS Principles encompasses "critical functions" as defined in FSB Guidance and is expanded to include activities, processes, services, and their relevant supporting assets the disruption of which would be material to the continued operation of the bank or its role in the financial system.

3.3 The context in which "critical business services" in the Guidelines and "critical functions" in MAS Notice 654 and FSB Guidance are applied is different. The policy objective of MAS Notice 654 and FSB Guidance is focused on resolution planning; to reduce financial stability risks when a systemically important bank is in distress and needs to restore its financial strength, be restructured or exited from the market in an orderly manner. On the other hand, the Guidelines are meant to apply to all FIs' business continuity processes which are operational in nature.

3.4 "Critical functions" in the BCBS Principles has a broader scope that encompasses both "critical business services" and "critical business functions" as defined in the Guidelines. In view of respondents' feedback that "business function" is a term that is commonly used by the industry and well understood, we have retained the term and its common industry meaning in the Guidelines. In addition, we have introduced "business service" in the Guidelines as there are specific expectations that apply only to "critical business services" such as on SRTO and dependency mapping.

Considerations in identifying critical business services and functions

3.5 Respondents sought clarification on who "the FI's counterparties and other participants in the financial ecosystem" encompass.

3.6 Respondents also sought further guidance on the factors that FIs should consider when identifying their critical business services and functions.

MAS' Response

3.7 "The FI's counterparties and other participants in the financial ecosystem" refer to other FIs that would be impacted when the relevant business service or function is unavailable. The Guidelines have been amended accordingly to reflect this.

3.8 Critical business services and functions are those that, if unavailable, could pose a risk to the FI's safety and soundness, or adversely impact its customers and other FIs.

(a) FI's safety and soundness: Examples of such adverse impact include damage to the FI's financial and liquidity position, loss of assets and revenue, loss of business and investments, inability to meet legal and regulatory obligations (including sanctions compliance), etc.

(b) FI's customers: When assessing the potential impact to customers, besides considering the number of customers that a business service supports, FIs

should also consider the type of customers (e.g. retail, corporate, interbank customers, etc.) and how they may be affected when the business service is unavailable.

(c) Other FIs that depend on the business service: FIs should also consider the extent of systemic impact on the financial sector at large. For instance, an FI appointed as the sole agent to settle USD cheque clearing obligations across the financial sector could impact multiple FIs when its service is unavailable. Multiple members and participants (including retail investors) of the exchange would be affected if the trading system is unavailable. Multiple FIs would also be impacted when the services of a benchmark administrator or payment networks provider is disrupted. The Guidelines have been amended to reflect this.

Granularity and frequency of reviewing critical business services and functions

3.9 Respondents sought guidance on the expected level of granularity to go into when defining their critical business services and functions, and the expected frequency of review for their critical business services and functions.

MAS' Response

3.10 In view of the differing sizes and complexity of business operations across different FIs, it is not possible to adopt a one-size-fits-all approach in applying the Guidelines. In defining critical business services and functions, FIs would be best placed to determine the appropriate level of granularity that is most suitable for their business context and environment, to effectively support their business continuity and recovery planning. To assist FIs in determining their critical business services, MAS has provided examples of business services in the Appendix of the Guidelines.

3.11 FIs should review their critical business services and functions at least annually, or whenever there are material changes to the people, process, technology, or other resources that support the delivery of critical business services.

Identifying critical business services

3.12 A respondent highlighted that it is possible that an FI does not have any time-critical business service, and whether that would in turn mean that it does not have any critical business service.

3.13 A few respondents requested for discretion to identify only the critical business functions, instead of both the critical business services and functions.

MAS' Response

3.14 The purpose of identifying critical business services is to take a customer-centric approach in driving their BCM, and to safeguard the continuous delivery of services to customers. It is possible that a business service is not time-critical, but still critical in other ways. Every FI should have at least one business service that is core to its business, and on which its viability depends. That business service would then be a critical business service in the FI.

3.15 Given the increasingly complex and interconnected operating environment of FIs, the conventional BCM approach of identifying and planning based on critical business functions may not be sufficient anymore. Interdependencies across functions could be missed, and this would impede the recovery of critical business services during a disruption. The identification of critical business services is a sound starting point for FIs to develop their dependency maps (refer to paragraph 5.14), allows FIs to better understand the interdependencies between business functions, and facilitates an end-to-end view of the complete set of processes and resources needed to deliver the business service.

Responsibilities of the overall manager

3.16 Respondents sought clarification on the responsibilities of the overall incident manager who is coordinating incident management across the affected functions and overseeing the resumption of the business service in the event of a disruption. They suggested segregating the responsibilities into two distinct roles, as the coordination of incident management and oversight of business service resumption are typically executed by different personnel.

MAS' Response

3.17 MAS agrees that the roles for incident management and oversight of business service resumption are distinct and could possibly be performed by different persons. FIs can have an overall coordinator to oversee their management of an incident and another appointed person to oversee the recovery and resumption of each critical business service.

4 Service Recovery Time Objective (SRTO)

Definition of SRTO

4.1 Respondents queried whether the SRTO refers to the time taken to fully restore the service, or to restore it to a minimum pre-determined capacity.

4.2 A respondent also sought guidance on how "business obligations" can be determined, and whether it is based on contractual obligations.

MAS' Response

4.3 SRTO refers to the target duration to restore a critical business service to a minimum service level that is sufficient to meet the FI's business obligations. This minimum service level should be pre-determined by the FI as part of its recovery planning. The Guidelines have been amended to reflect these points.

4.4 When assessing their business obligations, FIs can take into consideration their contractual obligations with customers, obligations to other FIs, and available industry service standards.

Establishing SRTOs for critical business services

4.5 Respondents suggested for MAS to establish standardised SRTOs for common business services across FIs.

4.6 A few respondents requested for discretion to continue with the identification and monitoring of RTOs for their critical business functions, in lieu of SRTOs for critical business services.

MAS' Response

4.7 SRTOs should be established based on the criticality of the FI's business services and the FI's business obligations, and these can differ across FIs, even for the same type of business services. Hence, it would not be practical or possible to standardise the SRTOs, even for common business services across FIs. Instead, FIs should derive the SRTOs of their business services from their own business impact analysis and based on their own business needs.

4.8 The SRTOs, along with the dependency maps, serve to facilitate an end-to-end view and planning of the recovery of an FI's critical business services. FIs should aim to first establish the SRTOs of their critical business services, use them to drive the recovery planning, and determine the RTOs of the underlying business functions.

Alignment of SRTO and Recovery Time Objective (RTO)

4.9 Respondents sought guidance on the alignment of "SRTO" and "RTO" in the Guidelines, and "RTO" used in MAS Notice 644 on Technology Risk Management ("MAS Notice 644").

4.10 Respondents highlighted that the criticality of the business functions supporting a critical business service would vary and there could be instances where the RTO of a supporting business function (e.g. loan initiation) could exceed the SRTO of a critical business service (e.g. loan services).

4.11 One respondent sought clarification on MAS' expectation in extreme events where an FI fails to meet the SRTOs.

MAS' Response

4.12 The term "RTO" needs to be considered with respect to the context in which it is used. "SRTO" and "RTO" in the Guidelines refer to the target duration to recover a critical business service and function respectively, whereas "RTO" in MAS Notice 644 refers to the target duration to restore a critical system.

4.13 FIs should also be cognizant of the relationships and interdependencies between the SRTO of a critical business service, the RTO of a critical business function, and the RTO of a critical system. For example, where a critical business service depends on a critical system, the FI should satisfy itself that the RTO established for the critical system will enable it to achieve the SRTO of the critical business service in the event of a disruption to the system.

4.14 A critical business service is typically supported by a number of business functions, and the RTOs of these business functions could vary depending on their criticality, and how they are needed to support the business service. In that regard, there may be exceptional cases where the RTO of a supporting business function could be longer than the SRTO of a critical business service. This could be the case when the business function is not in a critical path for the delivery of the critical business service. Hence, to guide them in deriving the SRTOs and RTOs, FIs should have a clear understanding of the end-to-end dependencies of their critical business services, including the underlying business functions and resources.

4.15 Some of these extreme events could have severe impact on the FIs and it is in the FIs' interest to have measures in place to address them. In the situation where an FI fails to meet the SRTO, MAS will assess if the FI has made adequate efforts to cushion the impact of the business service disruptions resulting from the events.

Partial disruption of a critical business service

4.16 Respondents sought clarification on the determination of thresholds for BCP activation during partial disruption of a critical business service. They highlighted that it would be challenging to define quantitative thresholds considering the varying disruption scenarios and their resultant impacts. Instead, respondents suggested that it is more important for FIs to have impact assessment criteria (e.g. nature of disruption, its severity, expected period of disruption, expected damage, impact on the safety and wellbeing of employees) and clear decision-making protocol for BCP activation to facilitate decision-making in a disruption.

MAS' Response

4.17 FIs may face situations where a critical business service encounters partial disruption (including intermittent or reduced performance) and the impact could worsen over time. To

enable timely response and recovery in such situations, FIs should, where possible, establish criteria for BCP activation. These could include quantitative thresholds[1] or the factors suggested, such as nature of disruption, expected damages, impact on safety and wellbeing of employees, in defining the criteria for BCP activation.

5 Dependency Mapping

Third parties supporting critical business services

5.1 Respondents highlighted that it may be challenging at times to implement measures such as requesting dedicated manpower from their third parties, conducting audits on the third parties, organising regular tests or joint tests with their third parties.

5.2 Other than conducting audits, regular tests, or joint tests with third parties, respondents sought clarification on whether alternative measures to obtain assurance, such as audits conducted as part of an industry certification process (e.g. ISO 22301 Security and Resilience – Business Continuity Management Systems), are acceptable.

MAS' Response

5.3 MAS recognizes that it is sometimes challenging to implement measures relating to third parties. The examples provided in paragraph 4.4 of the Guidelines are non-exhaustive and FIs should adopt a risk-appropriate approach to meet their business continuity objectives. The extent of measures to be implemented should be commensurate with the criticality of the third party and the impact on critical business services.

5.4 MAS agrees with respondents that audits performed as part of a certification process can be relied on to obtain the assurance on their third parties, provided that the audit is conducted by independent and competent assessors. The FI should also review and verify that the scope of the audit is adequate in providing the needed assurance over the third party's services.

Disruption, failure, or termination of third-party arrangements

5.5 Respondents sought clarification on whether by ensuring that their third parties can meet the SRTO (in paragraph 4.4 of the Guidelines), they would also have met MAS' expectation

[1] Examples of quantitative thresholds could include "more than X% of customers reported intermittent unavailability or transaction timeout of a critical business service for over a prolonged period (duration exceeding Y hours)", "more than X% of users reported reduction in processing capabilities of a critical system supporting a critical business service".

for FIs to have plans and procedures to address unforeseen disruption, failure, or termination of third-party arrangements (in paragraph 4.5 of the Guidelines).

5.6 Some respondents also highlighted challenges of pre-designating an alternative service provider in the event the primary service provider is unavailable to provide immediate support. These include incurrence of cost to engage specialised resources and operational challenges, such as the use of a proprietary system by the primary service provider.

MAS' Response

5.7 Paragraph 4.4 of the Guidelines focuses on ensuring that the FI's third parties have adequate measures in place to support the FI in achieving its SRTOs. On the other hand, paragraph 4.5 of the Guidelines is about the FI's own contingency measures to address scenarios where a third party is completely unavailable or unable to operate. Both sets of measures are needed to address different disruption scenarios and issues.

5.8 Pre-designating an alternative service provider is just one of the ways in which an FI can mitigate the risk of unavailability of its third-party service provider. FIs have the discretion to adopt measures most suitable to meet their business needs, and the measures should be informed and guided by their risk and impact assessments.

Interdependency risk posed by common third parties

5.9 Respondents highlighted that individual FIs have limited control over the recovery arrangement of common third parties such as financial market infrastructures and utilities providers. They would like to seek guidance on the expectation of implementing mitigating measures, to address the interdependency risks posed by the disruption of these services.

MAS' Response

5.10 MAS recognizes that there could be limited options available to FIs in addressing interdependency risks tied to financial market infrastructures and utilities providers. In such situations, FIs should have a process to accept the residual risks and work towards containing the impact if a disruption occurs. FIs should work with the relevant business units to put in place BCPs and other appropriate contingency measures to manage the disruption of such third parties, as far as possible.

Scope and granularity of dependency mapping

5.11 Respondents sought clarification on whether dependency mapping needs to be performed for critical business services, critical business functions, or only for third parties supporting critical business services. Another respondent queried if intra-group service providers should be included in the dependency map.

5.12 A respondent sought clarification on whether MAS' expectation of dependency mapping is the same as "mapping interconnections and interdependencies" defined in BCBS's Principles for Operational Resilience.

5.13 Respondents also sought guidance on the extent of granularity for their dependency map and requested an illustration of the dependency map.

MAS' Response

5.14 Dependency mapping should be performed for each critical business service to map out its end-to-end dependencies on the underlying business functions, processes and resources. This enables 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 their critical business services. The dependency mapping should include identifying the people, processes, technology, and other resources needed for the business service, including those from third parties. Third parties will also include intra-group service providers.

5.15 Dependency mapping in the Guidelines is aligned with the definition of "mapping interconnections and interdependencies" in the BCBS' Principles for Operational Resilience[2]. FIs could leverage their existing interconnections and interdependencies map that is prepared in accordance with the BCBS Principles.

5.16 Due to the nature, size, risk profile and complexity of each FI, there is no "one-size-fits-all" approach to dependency mapping. FIs should document the dependency map in a format and detail that best meet their needs in maintaining their BCM.

Structure of the Business Continuity Plans (BCPs)

5.17 A respondent sought clarification on the structure of the BCPs, particularly whether FIs can retain their existing business unit or business function-level BCPs, to meet the expectations articulated in the Guidelines.

MAS' Response

5.18 FIs may retain their existing business unit or business function-level BCPs, especially if the BCPs have been assessed and tested to be effective in supporting the timely recovery of their

[2] "Mapping interconnections and interdependencies" as defined in the BCBS Principles for Operational Resilience requires banks to identify and document the interconnections and interdependencies that the people, technology, processes, information, facilities, and the interconnections and interdependencies among them to deliver the bank's critical operations, including those dependent upon, but not limited to, third-party or intragroup arrangements.

business functions. In addition, FIs will also need to establish the SRTOs and dependency maps for their critical business services and ensure that the business unit and business function-level BCPs would enable them to achieve their SRTOs.

6 Concentration Risk

Mitigating concentration risk

6.1 Respondents sought guidance on the definition of a "zone" as used in the Guidelines, and the considerations in planning for concentration risk.

6.2 Another respondent sought guidance on how the cross-border support to deliver critical business services and functions could be implemented.

6.3 One respondent highlighted that it is challenging for small FIs or teams performing specialised functions to split their operations into multiple sites.

MAS' Response

6.4 A zone refers to an area or region that shares a similar risk profile, such that all the people, systems, data, and other key resources located within it would be affected by a disruption. FIs should consider the risk of concentration in a common geographical zone or service provider. For example, FIs could be exposed to concentration risk when they are highly dependent on one particular service provider for technology support.

6.5 An example of cross-border support was when during COVID-19, some FIs operating in multiple jurisdictions had switched to relying on the support of business functions in other jurisdictions to overcome the impact of lockdowns in affected regions. At the same time, cross-border support may also subject FIs to potential economic, social, political and legal/compliance risks that may be present in other jurisdictions. FIs should therefore examine and assess the potential risk implications before implementing cross-border support measures.

6.6 MAS recognises that some of the measures in paragraph 5.2 of the Guidelines are more relevant to larger FIs and may not be practical for smaller FIs, given their limited headcounts and resources. It is important that FIs assess their exposure to potential concentration risk, and put in place appropriate measures that are within their means and commensurate with the nature, size, risk profile and complexity of their business to manage the risks.

Work from home arrangements

6.7 Several respondents sought clarification on whether work-from-home arrangements could be considered a long-term recovery strategy. One respondent sought clarification on whether work from home arrangements could replace the need for an alternate office site.

MAS' Response

6.8 Work-from-home can be a long-term recovery strategy, as long as the FI is able to sustain its business operations and meet its business continuity objectives. To determine if work-from-home can replace the need for an alternate office site, FIs should perform an assessment on the capability of business units to fully work from home when the primary site is unavailable, including having access to the systems, equipment and other resources to effectively execute their work at home.

6.9 As work-from-home arrangements may entail changes to policies, operational processes, and use of equipment or IT systems that pose new risks, FIs should be cognizant of the resultant risks and put in place appropriate mitigating controls. FIs are also encouraged to refer to the paper on "Risk Management and Operational Resilience in a Remote Working Environment" jointly issued by MAS and The Association of Banks in Singapore (ABS) for risk management actions and examples of mitigating controls to manage risks arising from remote working arrangements.

7 Testing

Testing the BCM of critical business services

7.1 A respondent sought clarification on how the expectation on end-to-end BCM testing of a critical business service could be met, if the business service involved several business functions and third parties. The respondent asked if it could be split into separate tests.

7.2 Another respondent sought to understand what MAS' expectations with regard to testing for more extreme scenarios were.

7.3 Respondents also sought guidance on the type of tests that would be acceptable for critical business services.

MAS' Response

7.4 In the case where a critical business service is supported by multiple business functions and third parties, the BCM testing of the critical business service would require validating the recovery of the individual business functions and their interdependencies. This could be conducted within a single test or over separate tests.

7.5 Some examples of extreme scenarios could be a cyberattack that resulted in data corruption of both primary and secondary data centres, or a terrorist attack that resulted in prolonged unavailability of both staff and office premises. As the threats are constantly evolving, FIs should take reference from their ongoing threat monitoring and environmental scanning to formulate extreme scenarios for testing and determine the type of tests to be conducted to evaluate the effectiveness of the recovery strategies.

7.6 We have listed some examples of tests[3] in paragraph 7.3 of the Guidelines. FIs should select the type of tests that best meet their test objectives and determine the frequency and scope of these tests to commensurate with the criticality of the business services.

8 Audit

Scope and frequency of BCM audits

8.1 Respondents sought clarification on the interpretation of "scope and frequency of BCM audits to be commensurate with the criticality of the business services and business functions" in the Guidelines. A few respondents suggested to specify a minimum frequency (e.g. three years) for the BCM audit to be conducted, and suggested for the scope and frequency of BCM audits to also take into account the results of risk assessments, previous audit findings, and incidents within the FI and in other organisations.

8.2 Some respondents requested to substitute "BCM audits" with "BCM tests". One respondent sought clarification on whether audits conducted as part of industry certification process (e.g. ISO 22301 Security and Resilience – Business Continuity Management Systems) can be used to meet the BCM audit expectations in the Guidelines.

MAS' Response

8.3 MAS expects FIs to conduct a BCM audit at least once every three years. The scope of the audit should cover the FI's overall BCM framework and the BCM of each of its critical business services. The audit should assess the adequacy and the effectiveness of the FI's BCM. In the BCM audit, the FIs should also examine the higher risk areas that they have identified from the risk assessment, previous audit findings, and relevant incidents. The Guidelines have been amended to reflect these points.

8.4 BCM audits provide an independent assessment on the adequacy and effectiveness of the BCM framework, including the quality and robustness of the BCM testing conducted. In this regard, BCM tests are not substitutes for BCM audits.

8.5 FIs can rely on industry certification audits to meet the BCM audit expectations in the Guidelines. However, FIs should also be cognizant that the industry certification may not necessarily cover all areas in the Guidelines, in which case the audit will only satisfy the Guidelines partially. To cover the Guidelines fully, FIs may have to extend the scope of the audit, or conduct additional audits, to cover those areas not included under the industry certification.

[3] Types of tests could range from basic call-tree activation, 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.

Personnel conducting BCM audits

8.6 Respondents sought clarification on the type of qualification that the independent auditor should possess.

8.7 Respondents asked if the internal auditor or independent unit in the second line-of-defence can be allowed to conduct the BCM audit.

MAS' Response

8.8 When appointing the auditors, FIs should assess their qualifications and competencies in BCM and conducting audits, by taking into account their working experiences and professional certifications (e.g. industry recognised BCM certifications).

8.9 The BCM audit can be conducted by the FI's internal or external auditors, or personnel from a unit/department in the FI who possesses the requisite BCM knowledge and expertise and is independent of the unit or function responsible for the BCM of the FI.

9 Incident and Crisis Management

Incident notification to MAS

9.1 Respondents suggested for MAS to specify a timeframe for reporting of incidents where business operations are, or will, be severely disrupted, or when the BCP is activated, or going to be activated. One respondent also highlighted that the interpretation of a severe incident could vary across FIs and sought further guidance on what constitutes a severe incident that should be reported to MAS.

MAS' Response

9.2 MAS acknowledges that providing a reporting timeframe will help to provide clarity on the time by which FIs need to report an incident. The Guidelines have been updated to indicate that FIs should notify MAS as soon as possible, but not later than one hour upon the discovery 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.

9.3 An incident should be reported to MAS if it is one that is severe and has widespread impact on an FI's operations, or materially impacts the FI's service to its customers. Each FI should establish a set of criteria to guide its impact assessment on what constitutes a severe incident that should be reported to MAS, and the criteria should be aligned with the FI's incident management and reporting framework. The criteria should be endorsed by the senior management.

10 Responsibilities of Board and Senior Management

Measurable goals and metrics to assess the FI's business continuity preparedness

10.1 One respondent requested for examples of measurable goals and metrics that can be used to assess the FI's overall business continuity preparedness, as described in the section on responsibilities of Board and senior management.

MAS' Response

10.2 Examples of measurable goals and metrics will include the success rates of BCM tests, the ability to achieve the SRTOs and RTOs during BCP drills, recovery times of critical business services/functions during incidents, participation rates of BCM awareness programmes, assessment results from staff training on BCM, and BCM audit results (e.g. number of findings, criticality of findings).

BCM attestation

10.3 Respondents sought clarification on whether global FIs are able to leverage established reporting frameworks to the Board as a form of BCM attestation.

MAS' Response

10.4 The annual attestation to the Board should encompass (i) assessment of the state of the FI's BCM preparedness, (ii) the extent of its alignment with the Guidelines, and (iii) key issues requiring attention by the Board, such as significant residual risk. Global FIs can leverage their established reporting frameworks, so long as the frameworks cover these areas and can meet the objectives set out.

RESPONSE TO FEEDBACK RECEIVED ON SECOND CONSULTATION - PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

JUNE 2022

Monetary Authority of Singapore