

CONSULTATION PAPER

P004 - 2019

March 2019

Proposed Revisions to Guidelines on Business Continuity Management

MAS

Monetary Authority of Singapore

Contents

| | | |
|---|--|----|
| 1 | Preface | 3 |
| 2 | Proposed Revision to Guidelines on BCM | 4 |
| 3 | ANNEX A – List of Questions | 10 |
| 4 | ANNEX B – Revised Guidelines on BCM..... | 11 |

1 Preface

1.1 The Monetary Authority of Singapore (MAS) first issued the Business Continuity Management (BCM) Guidelines in 2003. These guidelines were supplemented by additional guidance on pandemic and physical security measures in 2006.

1.2 Since then, the threat landscape has changed. For example, cyber-attacks have increased in scale and frequency and the threat of terrorism has heightened. Financial institutions (FIs) should therefore continue to strengthen their ability to mitigate the potential impact of any attacks by identifying potential vulnerabilities and developing effective recovery plans. FIs also have to appreciate the interdependencies between people, business processes and technology in the performance of their various business functions.

1.3 The proposed changes are part of MAS' efforts to help FIs strengthen their resilience to disruptions. FIs will be expected to adopt the Guidelines within a year following its publication. The revised Guidelines will also supersede MAS Circular SRD BCM 01/2006. MAS invites interested parties to submit their views and comments on the Guidelines on BCM. All comments should be submitted to MAS by **8 April 2019**.

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, or (ii) their identity, or both, to be kept confidential, please expressly state so in the submission to MAS. 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.

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

1.5 For non-electronic submissions, you may submit your comments to the following address –

Technology Risk and Payments Department
(Attention: Payments & Infrastructure Division)
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Fax: (65) 62203973

2 Proposed Revision to Guidelines on BCM

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

Critical Business Functions and Business Continuity Objectives

2.2 The existing Guidelines on BCM set out MAS' expectations of how an FI is to identify business functions that are critical and prioritise them for recovery in a disruption. Such functions could include completing payment instructions, clearing and settling transactions, and fulfilling end-of-day funding and collateral obligations.

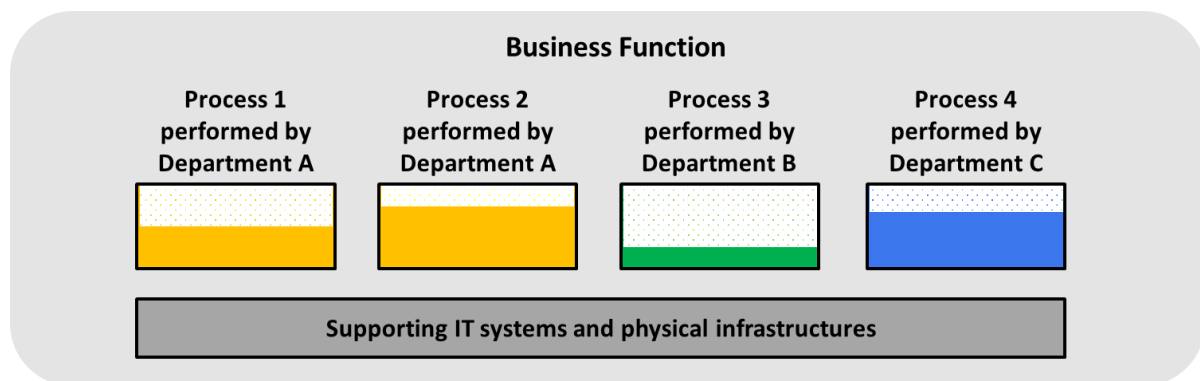
2.3 In general, FIs have been observed to establish business functions, and conduct BCM planning, along organisational lines (e.g. by department or unit), with the focus being on the business processes performed by individual organisational units.


2.4 As IT systems and business processes become more complex, a service may depend on an increasing number processes performed by several different units to be delivered. Taking a silo approach may result in omissions in considering dependencies between processes, which would impact the recovery of the service in the event of a disruption.



2.5 MAS proposes to revise the definition of business function to a service that an FI ultimately provides to its customers. For this service to be delivered, it will likely require a number of business processes to be performed. For example, the "securities trading" business function of a brokerage could entail the following processes: (i) Trade Initiation; (ii) Trade Execution; (iii) Trade Capture; (iv) Trade Validation; (v) Trade Agreement; (vi) Trade Settlement; and (vii) Trade Reconciliation. Each process, in turn, requires specific resources and expertise (e.g. IT systems, personnel) to be performed.

2.6 As in the current Guidelines, an FI should define recovery time objectives (RTO) and recovery point objectives (RPO) at the business function level. In addition, an FI should set a minimum performance level for each business function. The minimum performance level, RTO and RPO, would constitute the business continuity objectives for each business function. The business continuity objectives for a particular business function should be supported by all systems and processes that the function depends on.

2.7 In addition, an FI may face scenarios where the performance of a business function is intermittent and the root cause may not be immediately apparent. To cater for such scenarios, an FI should establish monitoring capabilities that will enable prompt detection of reduced or intermittent service availabilities and clearly articulate triggers for the activation of contingency plans. These triggers could take reference from the minimum performance level for a given business function.



 Denotes the degree to which each individual business process needs to be recovered in order to achieve the minimum performance level for the business function overall.

Question 1. MAS seeks comments on the definition of "business function".

Responsibility of Board and Senior Management

2.8 An FI's risk culture plays an important role in influencing the actions and decisions taken by individuals within the institution and in shaping the institution's attitude toward business continuity. As such, we will place greater emphasis on the Board of directors ("Board") and senior management to demonstrate their leadership and commitment in building an organisational culture that embeds business continuity as part of an FI's business-as-usual ("BAU") considerations and day-to-day risk management.

2.9 MAS continues to expect the Board and senior management to be ultimately responsible for the business continuity of their FI. To achieve this effectively in the current threat environment, we propose that the Board take on additional responsibilities to:

- (a) Review and endorse, at least annually, the FI's BCM, as well as ensure that the framework consists of comprehensive policies, processes and procedures, appropriate oversight and escalation elements;
- (b) Review and endorse, at least annually, the FI's critical business functions, business continuity objectives and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place; and
- (c) Satisfy itself that adequate resources, including budget, technology, and staff are allocated to facilitate the implementation of an effective BCM.

2.10 For effective governance and accountability, we propose that senior management should:

- (a) Implement effectively the FI's BCM through established policies, processes and procedures. The roles and responsibilities of personnel involved in the FI's BCM should be clearly defined and documented;
- (b) Review, at least annually:
 - (i) The list of critical business functions identified and the appropriateness of their respective business continuity objectives;
 - (ii) The key assumptions underlying the various BCPs;
 - (iii) The extent to which the FI had tested their BCPs and crisis management plans to assure itself that the FI's business continuity objectives can be achieved in a disruption;

- (iv) Whether the areas of improvement identified by BCM tests are being appropriately addressed; and
 - (v) The adequacy of the FI's BCM training program for new and existing staff.
- (c) Participate actively in the FI's BCM tests.
- (d) Provide an annual attestation to the Board stating the BCM preparedness of the FI and the extent of its alignment with the Guidelines.

2.11 BCM is part of an FI's broader operational resilience. Where an FI sets up a committee to oversee its BCM, the committee should thus be led by a senior management member with responsibility over its overall risk (e.g. the Chief Risk Officer).

2.12 The proposed Guidelines articulate MAS' expectations that an FI should have a crisis management team (CMT) that comprises senior management representatives to oversee its crisis management activities, such as the recovery of business functions during a severe disruption, and the implementation of processes to achieve the FI's business continuity objectives during a severe disruption. An FI should have clear triggers and processes to activate its CMT (e.g. the escalation protocol and the means through which the CMT will be convened).

2.13 An FI should review the adequacy of training for CMT members at least annually and ensure that they are competently prepared for their roles and responsibilities.

Question 2. MAS seeks comments on the roles and responsibilities proposed for the Board and senior management.

Business Continuity Plans

2.14 Notwithstanding that BCPs are well-established in FIs, not all FIs have developed end-to-end BCPs for a given business function. MAS' view is that having an overarching BCP for a business function (i.e. the service ultimately being provided to customers) is a better approach to BCM and provides better clarity to an FI's management and customers. In addition to making interdependencies more explicit, it will also facilitate recovery monitoring.

2.15 The proposed Guidelines will expect FIs to have in place end-to-end business continuity plans for each service that is delivered to their customers, thereby drawing out any internal or external dependencies. We propose for FIs to review and, where necessary, enhance the robustness and comprehensiveness of their BCPs by covering the full recovery process for a given business function from immediate response to the resumption of business functions to minimum levels, and the subsequent restoration to BAU levels. The need for such end-to-end BCPs would be in addition to the need for BCPs at the unit, or department, level that relate more to individual processes.

2.16 The efficacy of a BCP begins with a comprehensive risk assessment. Hence an FI should ensure their risk assessment processes identify plausible disruptions and assess their risks to the institution, including the impact on the availability or functionality of staff, physical/IT infrastructure and third-party vendors. There should also be a process to identify and understand the various internal and external interdependencies (e.g. staff, systems and equipment). Using these, an FI should develop and/or update the BCP (annually or earlier if there was material changes).

2.17 An FI should establish a formal training programme to ensure that all relevant personnel are familiar with their roles and responsibilities in relation to a BCP. The adequacy of training for all relevant staff should also be reviewed at least annually.

Question 3. MAS seeks comments on the proposed scope of a BCP.

Testing and Audit

2.18 Testing is crucial in validating an FI's BCM preparedness as it ensures an FI's response and recovery arrangements are effective and developed based on sound understanding of existing systems and processes.

2.19 MAS continues to expect an FI to conduct different types of testing to gain the confidence that they will be able to continue to operate reliably, responsively, and efficiently as planned. Specifically, an FI should, at minimum, conduct the following annually:

- A crisis management and communications exercise involving all CMT members and their alternates; and
- A test relating to the BCP for each critical business function.

2.20 In addition, we propose for an FI to conduct BCM audits through a unit independent of the staff involved in the planning and execution of the BCM itself (e.g. internal audit).

2.21 An FI should also check that the scope of BCM audits is sufficiently comprehensive and includes all critical business functions. A BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The BCM audit plan should be approved by the FI's Audit Committee. The frequency of BCM audits should be commensurate with the criticality of the business functions. Consequently, an FI should establish follow-up processes to track and monitor BCM audit issues, as well as escalation processes to notify the relevant senior management of key BCM audit issues. The FI should submit the BCM audit reports to MAS upon request.

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

Question 4. MAS seeks comments on the proposed type and frequency of BCM tests.

Question 5. MAS seeks comments on the expectation of conducting regular BCM audits.

Question 6. MAS seeks comments on any other aspects of BCM that warrant further guidance from MAS.

3 ANNEX A – List of Questions

| | |
|---|---|
| Question 1. MAS seeks comments on the definition of “business function”. | 5 |
| Question 2. MAS seeks comments on the roles and responsibilities proposed for the Board and senior management..... | 7 |
| Question 3. MAS seeks comments on the proposed scope of a BCP..... | 8 |
| Question 4. MAS seeks comments on the proposed type and frequency of BCM tests..... | 9 |
| Question 5. MAS seeks comments on the expectation of conducting regular BCM audits. | 9 |
| Question 6. 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

1.1 The smooth delivery of financial services typically depends on a complex network of systems and processes. As part of overall risk management, a financial institution (FI) is expected to have controls in place to minimise the occurrence of service disruptions, including identifying potential single points of failure early on and eliminating them where possible.

1.2 Nonetheless, disruptions can still occur despite an FI's best efforts. In such situations, MAS expects an FI to have plans and systems in place to minimise the impact of disruptive events on the performance of its business functions.

1.3 The Guidelines on Business Continuity Management (BCM) provides guidance on establishing plans to ensure that business functions can be promptly resumed following a disruption.

1.4 The Guidelines do not affect, and should not be regarded as a statement of, the standard of care owed by FIs to their customers. The extent and degree to which an FI implements the Guidelines should be commensurate with the nature, size and complexity of its business operations. In supervising an institution, MAS will assess the quality of its Board of directors ("Board") and senior management oversight and governance, internal controls and risk management. Particular attention will be paid to an FI's critical business functions.

1.5 The practices espoused in the Guidelines are not intended to be exhaustive or override any legislative provisions. They should be read in conjunction with the provisions of the relevant legislation, the subsidiary legislation made under the relevant legislation, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

1.6 These Guidelines supersede the BCM Guidelines published in June 2003, and the circular, "Further Guidance on BCM", issued in January 2006.

2 Definitions

| Terminology | Definitions (as used in this document) |
|--------------------------------------|---|
| Business Continuity Management (BCM) | An overarching framework that includes policies, standards, processes and procedures that provides for continuous functioning of the FI during operational disruptions. It should be commensurate with the FI's nature, scale and complexity of business activities. |
| Business Continuity Plan (BCP) | A plan that sets out the process to restore a business function or unit in the event of a disruption. A BCP would identify the systems and people needed to restore the function/unit, where relevant, and include end-to-end procedures to address various types of disruptions. |
| Business Impact Analysis (BIA) | The process of measuring the loss (both financial and non-financial) to an FI in the event that its business function or unit is disrupted. A BIA is useful in identifying the recovery priorities, recovery resource requirements, recovery strategies and critical staff. |
| Business Function | A 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. |
| Disruption | A disruption occurs when the normal performance of a business function is degraded, resulting in impact to customers. A disruption is not limited to a complete non-availability of a business function, and would include intermittent service availability as well. |
| Minimum Performance Level | In relation to a business function or unit, the minimum level of output that an FI will aim to recover to in its initial phase of recovery following a business disruption. |
| Recovery Time Objective (RTO) | RTO comprises: (1) the duration of time from the point of business disruption, to the point of declaring the activation of BCP(s) for business functions or units and interdependencies, and (2) the duration of time from the BCP activation to the point when the specific business function or unit is recovered to its Minimum Performance Level. |
| Recovery Point Objective (RPO) | The maximum tolerable data loss and is measured from the point of the last data backup. |
| Residual Risk | The risk that a business function will not be available for an extended period of time despite the relevant business continuity measures being put in place. |

3 Critical Business Functions and Business Continuity Objectives

Business Function

3.1 A business function refers to a service provided to customers of an FI. For this service to be delivered, it will likely require a number of business processes to be performed. For example, the “securities trading” business function of a brokerage could entail the following processes: (i) Trade Initiation; (ii) Trade Execution; (iii) Trade Capture; (iv) Trade Validation; (v) Trade Agreement; (vi) Trade Settlement; and (vii) Trade Reconciliation. Each process, in turn, requires specific resources and expertise (e.g. IT systems, personnel) to be performed.

3.2 In a crisis, it might not be practical to recover *all* business functions at the earliest opportunity. FIs should therefore identify business functions that are critical to them based on the potential loss (both financial and non-financial) to them should these functions be disrupted. The process through which one determines the relative importance of business functions is commonly known as business impact analysis (BIA). In determining relative importance, FIs should also consider the impact of a disruption of their business function on other FIs (e.g. other participants of a payment system) and their customers. A BIA¹ should be performed at least annually, and whenever there are material changes to the business functions performed by an FI.

Business Continuity Objectives

3.3 FIs should determine the business continuity objectives for each business function identified. These should be consistent with the level of residual risk that the Board is willing to accept. Business continuity objectives comprise the following:

- (a) The minimum performance level, which must be recovered by the RTO, that is acceptable²; and
- (b) The RTO and RPO for each business function, which would in turn translate to RTOs and RPOs for all relevant processes and systems that are required for the minimum performance level to be achieved.

¹ While the focus here is on business functions, FIs should also conduct BIA and establish business continuity objectives at the unit-level.

² The definition of “service level” will vary depending on the type of service being provided.

3.4 FIs should ensure that the minimum performance level for each business functions¹ is suitably defined, clear and measurable.

3.5 FIs may face scenarios where the performance of a business function is intermittent. This may arise, for example, due to intermittent network connectivity or faulty hardware, and the root cause may not be immediately apparent. To manage such scenarios, FIs should have monitoring capabilities that will enable prompt detection of reduced or intermittent service availabilities and clearly articulate triggers for the activation of contingency plans (e.g. fail over to a secondary data centre). These triggers should take reference from the minimum performance level for a given business function.

4 Responsibility of Board and Senior Management

4.1 The Board and senior management are ultimately responsible for the business continuity of their FI. A prolonged disruption in the performance of critical business functions could significantly impair an FI's reputation, its financial well-being, or the interests of its customers. The Board and senior management should therefore establish strong governance and effective policies and procedures to address a wide range of disruptive events including, but not limited to loss of staff, equipment and infrastructure (both IT and physical). Due consideration should also be paid to the potential loss of services provided by third parties to the FI.

4.2 The Board and senior management should demonstrate their commitment to build an organisational culture that embeds business continuity as part of an FI's business-as-usual ("BAU") risk management.

4.3 The Board³ should:

- (a) Review and endorse, at least annually, the FI's BCM, as well as ensure that the framework consists of comprehensive policies, processes and procedures, appropriate oversight and escalation elements;
- (b) Review and endorse, at least annually, the FI's critical business functions, business continuity objectives⁴ and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place; and
- (c) Satisfy itself that adequate resources, including budget, technology, and staff are allocated to facilitate the implementation of an effective BCM.

³ 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 overseas incorporated institutions in Singapore, the roles and responsibilities specified for the Board can be performed by the relevant function responsible for BCM at Group/Global level.

⁴ Please refer to Para 3.5 of this document for the definition of business continuity objectives.

4.4 Senior management should:

- (a) Implement effectively the FI's BCM through established policies, processes and procedures. The roles and responsibilities of personnel involved in the FI's BCM should be clearly defined and documented⁵;
- (b) Review, at least annually:
 - (i) The list of critical business functions identified and the appropriateness of their respective business continuity objectives;
 - (ii) The key assumptions underlying the various BCPs;
 - (iii) The extent to which the FI had tested their BCPs and crisis management plans to assure itself that the FI's business continuity objectives can be achieved in a disruption⁶;
 - (iv) Whether the areas of improvement identified by BCM tests are being appropriately addressed; and
 - (v) The adequacy of the FI's BCM training programme for new and existing staff.
- (c) Participate actively in the FI's BCM tests.
- (d) Provide an annual attestation to the Board stating the BCM preparedness of the FI and the extent of its alignment with the Guidelines. The attestation should also be provided to MAS as and when required.

4.5 BCM is part of an FI's broader operational resilience. Where an FI sets up a committee to oversee its BCM, the committee should be led by a senior management member with responsibility over its overall risk (e.g. the Chief Risk Officer).

⁵ FIs, especially those with multiple lines of businesses and services, are encouraged to have a dedicated BCM function sufficiently resourced for enterprise-wide coverage of BCM and the effective implementation of the programme.

⁶ Please refer to Section 6 of this document.

Crisis Management

4.6 An FI should have a crisis management team (CMT) that comprises senior management representatives to oversee its crisis management activities, such as the recovery of business functions during a severe disruption, and the implementation of processes to achieve the FI's business continuity objectives during a severe disruption. An FI should have clear triggers and processes to activate its CMT (e.g. the escalation protocol and the means through which the CMT will be convened).

4.7 An FI should develop a crisis management plan to support the CMT's decision making process. The crisis management plan should:

- (a) Set out the criteria and processes for CMT activation;
- (b) Define clearly the roles and responsibilities of CMT members and their alternates;
- (c) Include an agenda to guide discussions and the maximum time allocated to assess and activate the recovery arrangements for different types of disruption, including scenarios where performance of the critical business function is intermittent, in order to achieve RTO; and
- (d) Identify external stakeholders and their expected involvement in managing a disruption; and
- (e) Set out a potential work routine in the event that the duration of the crisis is prolonged

4.8 As crisis management is usually complex and time critical, an FI should regularly assess the need for additional tools to more effectively manage a crisis. These include systems that enhance an FI's situational awareness and monitoring to support the decision making of CMT.

4.9 An FI should review the adequacy of training for CMT members at least annually and ensure that they are competently prepared for their roles and responsibilities.

5 Business Continuity Plans

5.1 A BCP is a formal document that captures the process and procedures that are needed to fulfil a set of business continuity objectives following a disruption. BCPs are typically established at the organisational unit level (e.g. by department or unit), but should also be established at the business function level. BCPs should cover the full recovery process: immediate response to the resumption of output to minimum performance levels, and the subsequent restoration to BAU levels. This chapter focuses on business functions, but the same principles apply to unit-level BCPs.

Risk Assessment

5.2 Disruptions could be caused by malicious acts (e.g. cyber-attack, terrorism), natural occurrences (e.g. floods, pandemics) or accidents (e.g. electricity outages, failure of individual system components). Disruptions typically arise due to the diminished availability or functionality of one or more of the following factors that the business function depends on: personnel, physical infrastructure and/or IT components⁷. A disruption could also occur due to the failure of a key third-party service provider⁸.

5.3 An FI's risk assessment processes should identify possible causes of disruptions, and their potential impact on the institution, including but not limited to, the factors mentioned above. A BCP should contain measures to address the diminished availability or functionality of any factor through prompt replacement or process changes.

5.4 While a BCP for a given business function could be largely the same regardless of the cause of the disruption, an FI should be mindful that specific scenarios could impose constraints on its recovery options. For example, a cyberattack could result in the data in both primary and secondary data centres being destroyed or manipulated. Similarly, a terrorist attack could impede the ability of staff to relocate to an alternate site due to security or other physical restrictions.

5.5 In this regard, an FI should develop BCPs that can address a broad range of plausible scenarios from wide-area disruptions to pandemics. For example, the primary and secondary

⁷ This includes, but is not limited to, all IT software and hardware such as firewalls, routers, switches, servers, storage and processors.

⁸ This includes, but is not limited to, telecommunication providers, electricity providers and outsourced service providers.

sites of critical business functions should not rely on the same substation for electricity. FIs with sufficient scale could also operate from multiple locations such that staff and equipment located at a secondary site will be sufficient to allow an FI to continue performing a business function even when the primary site is completely unavailable.

5.6 FIs should establish a process to monitor news or developments on incidents that could have a downstream impact on their business functions. Lessons learned from its own near-misses, as well as incidents at other FIs or industries, can be used to enhance the institution's understanding of plausible causes of disruptions. In addition to institution-specific disruptions, an FI should also have the plans to deal with a general pandemic outbreak in a manner consistent with the guidance issued by the Ministry of Health.

Interdependencies

5.7 An FI should have processes to identify and understand the various internal and external interdependencies (e.g. staff, systems and equipment) so as to avoid gaps in business continuity planning that could hinder the effective and safe recovery of its business functions.

5.8 Where recovery arrangements rely on other stakeholders, such as intra-group partners and third party vendors, formal service level agreements (SLAs) should be established and the appropriate redundancies agreed upon. This would include setting specific and measurable recovery expectations (e.g. RTOs), mutual participation in testing and review of SLAs on a regular basis. FIs are encouraged to share their business continuity objectives with key stakeholders to mitigate the risk of mismatched expectations. An FI should proactively assess the resilience of these stakeholders and involve them in its BCM exercises, where appropriate.

5.9 Some interdependency risks are beyond an FI's direct control to mitigate completely (e.g. unavailability of telecommunications networks, etc.), but reasonable steps should still be taken to provide assurance that key service providers are capable of supporting their businesses even in disruptions.

Restoration of Business Functions

5.10 In order to restore relevant business functions to minimum service levels within the stipulated RTO, FIs should have robust processes to manage incidents. This would include involving subject matter or business process experts⁹ where relevant. As the performance of a business function would involve several parties within an FI, an overall incident manager should be clearly identified.

5.11 FIs should notify MAS promptly¹⁰ when a critical business function is disrupted, providing information on the assessed impact on its customers and the actions that have been taken (alternative service channels, media engagement, etc.).

5.12 FIs should define a reasonable target timeframe for their business functions to be restored to BAU levels under the various disruption scenarios that they plan for. The relevant processes needed to achieve that target timeframe should be clearly articulated in the BCP.

Communications

5.13 In crisis communications, FIs should aim to be proactive, transparent and factual, with a view to maintain customer confidence and safeguard the interest of their customers. FIs should establish crisis communication plans that include the following:

- (a) List of all stakeholders (e.g. customers, media, regulators) that would need to be informed in a disruption of each business function with target timelines. Primary and secondary means of communication with these stakeholders should be identified and established to confirm that the information communicated is accurate and provided in a timely manner;
- (b) Pre-drafted media statement templates to cater for different scenarios so as to expedite public communications during a crisis; and
- (c) List of designated spokespersons (e.g. CEO, deputy CEO) and their alternates.

⁹ These include experts from the respective risks areas (e.g. corporate security and cyber security)

¹⁰ FIs should notify MAS through their review officers or the MAS BCM Hotline.

5.14 Relevant portions of these communication plans should be aligned with crisis communication protocols established by industry associations so that there is consistent messaging to the public in a wide-spread disruption.

Proper Documentation and Maintenance

5.15 The BCP should be properly documented to comprehensively cover all processes and procedures, as well as to clearly describe the tasks, roles and responsibilities of relevant personnel and their identified alternates.

5.16 The following (non-exhaustive) components are expected to be included in the BCP:

- Planning assumptions;
- Business continuity objectives
- Identified recovery staff and alternates;
- Detailed procedures, according to a timeframe, performed by staff;
- Procedures to retrieve vital records¹¹;
- Notification procedures, e.g. call trees procedures;
- Information on the recovery site;
- Coordination with external dependencies and parties (including authorities, etc.); and
- Related information or references on IT recovery, such as critical applications and databases and their RTOs/RPOs.

5.17 Given the various factors required to perform a business function, several units within the FI are likely to play a role in the BCP of a given business function. It is therefore important for a lead unit to be responsible for ensuring that the BCP remains current. The BCP should be updated annually, or when there are material changes to businesses.

5.18 An FI should establish a formal training programme to ensure that all relevant staff are familiar with their roles and responsibilities in relation to a BCP. The adequacy of training for all relevant staff should also be reviewed at least annually.

¹¹ This refers to important records of business information that are required to provide a business function. Examples of vital records are, but not limited to: customer contact lists, database back-ups, transaction records and contracts.

6 Testing and Audit

6.1 Testing is crucial in validating an FI's BCM preparedness as it ensures an FI's response and recovery arrangements are effective and developed based on a sound understanding of existing systems and processes.

6.2 An FI should have a formal testing programme to systemically validate their ability to achieve their business continuity objectives in the event of a disruption. The testing programme should comprise a process to regularly and meaningfully test¹² all aspects of a business function's BCP, as well as an FI's overall crisis management plan.

6.3 The tests conducted could range from basic call-tree activation and failover of specific applications and IT components, to more complex exercises such as:

- Failing over to an alternate data centre;
- Operating from a disaster recovery site for a defined duration to gain assurance that the infrastructure can fully support business-as-usual capacity;
- Operating with reduced headcount or back-up staff;
- Operating in the absence of a key third party service provider;
- Relying on power from onsite generators for a prolonged period; and
- Restoring data from back-up media.

6.4 The type and frequency of exercises should be commensurate with the scale and complexity of the FI, with particular attention being paid to critical business functions. At the minimum, an FI should conduct the following annually:

- A crisis management and communications exercise involving all CMT members and their alternates; and
- A test relating to the BCP of each critical business function.

6.5 An FI should use appropriate quantitative and qualitative metrics to ensure that there is consistency in measuring the extent to which the various business continuity objectives are met for each test. These metrics include the ability to meet RTOs and RPOs, the

¹² Testing encompasses exercises, rehearsals, etc. In this document, the words "test" and "exercise" are used interchangeably.

percentage of staff accounted for within a specified period from the point of a call-tree activation, etc.

6.6 Senior management and staff with BCM responsibilities should participate in all relevant tests. Designated alternates should also participate in these tests so that they are adequately prepared to take over the primary staff's roles if necessary.

Testing Administration, Documentation and Follow-up

6.7 While executing tests, an FI should put in place measures to prevent staff from mistaking test-related materials for that of an actual incident. All aspects of testing, e.g. test objectives, scope, participants, results and follow-ups, should be properly documented and action plans established to address the gaps identified in the tests. The gaps should also be included in subsequent tests to validate that the remediation measures are effective.

Industry-wide Exercises

6.8 FIs are strongly encouraged to participate in exercises such as those organised by government agencies, regulatory bodies, industry associations and Financial Market Infrastructure operators. Doing so would strengthen coordination among institutions and enhance and increase confidence in the sector's overall business continuity capability.

6.9 Industry-wide exercises are important because they allow FIs, financial utility providers¹³, government agencies and regulators to validate their response plans in light of the external interdependencies they may have on each other. Examples of such exercises include:

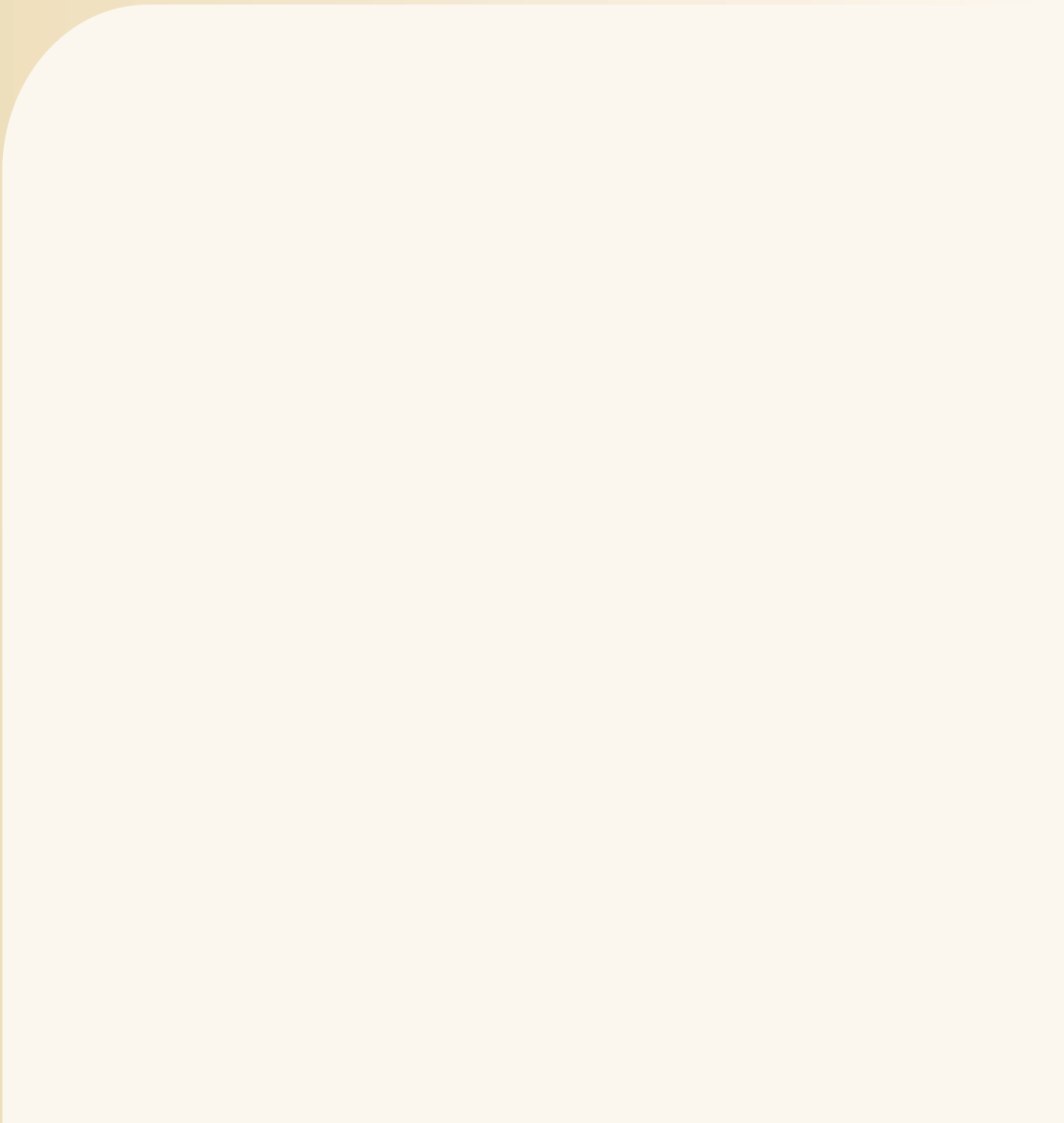
- (a) Business continuity exercises organised by the Association of Banks in Singapore;
- (b) Contingency tests organised by the Singapore Automated Clearing House;
- (c) MEPS+ contingency exercises organised by the Monetary Authority of Singapore;
and
- (d) Business continuity testing by the Singapore Exchange.

¹³ Financial utility providers are organisations that provide specialised financial services such as cheque clearing and settlement.

Audit

6.10 An FI should develop an audit process for greater assurance that their BCM is effective. Such audits should be conducted by a unit independent of the staff involved in the planning and execution of the BCM itself (e.g. internal audit).

6.11 An FI should also ensure that the scope of BCM audits is sufficiently comprehensive and includes all critical business functions. A BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The BCM audit plan should be approved by the FI's Audit Committee. The frequency of BCM audits should be commensurate with the criticality of the business functions. Consequently, an FI should establish follow-up processes to track and monitor BCM audit issues, as well as escalation processes to notify the relevant senior management of key BCM audit issues. The FI should submit the BCM audit reports to MAS upon request.



Monetary Authority of Singapore