MAS Revised Guidelines on Business Continuity Management ("BCM")

Following two rounds of public consultation, the MAS has issued a revised Guidelines on BCM on 6 June 2022 with the view to helping Financial Institutions ("FIs") build resilience against service disruptions and to factor in emerging threats from terrorism-related security concerns and pandemic outbreaks. The new guidelines supersede the previous version that was published in June 2003 and the circular titled "Further Guidance on BCM" issued in January 2006. FIs should meet the new guidelines and establish a BCM audit plan by **6 June 2023**. The first BCM audit should be conducted by **6 June 2024**. MAS may review an FI's BCM as part of its supervision, during which particular attention will be accorded to an FI's BCM Critical Business Services[1].

The new guidelines highlight best practices that FIs should adopt and the extent and degree of implementation should be commensurate with the respective FIs' nature, size, risk profile, and complexity of business operations.

1. Critical Business Services and Functions

In the event of a disruption, FIs should prioritise the recovery of business functions and services based on their criticality and determine the appropriate recovery strategies and allocation of resources. FIs should consider the impact of the unavailability of such business services and functions on:

(i) the FI's safety and soundness;
(ii) the FI's customers, based on the number and profile of affected customers as well as how they are impacted; and
(iii) other FIs that depend on the business service.

FIs should ensure clear accountability and responsibility for the business continuity of their critical business services and appoint personnel to oversee the recovery and resumption of each critical business service in the event of a disruption.

Service Recovery Time Objective ("SRTO")[2]

FIs should establish a SRTO for each critical business service so that they can be guided on the prioritisation of resources and decision-making during a crisis. The SRTO is a time-based metric that provides clarity on the expected recovery timelines for each business service. In establishing the SRTO, FIs are expected to:

- consider their obligations to customers and other FIs that are dependent on its service; and
- implement recovery strategies (e.g., activation of alternate sites) to allow them to achieve the STRO.

FIs should also set out clearly defined criteria for Business Continuity Policy ("BCP") activation when a critical business service encounters partial service disruption; this could be in the form of intermittent or reduced performance of services. This will allow the FIs to be better prepared to activate its BCP in a timely manner to avoid a situation where the service degradation deteriorates to a critical level.

[1] "Critical Business Services" means a business service which, if disrupted, 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.

[2] "Service Recovery Time Objective" refers to the target duration of time to restore a specific business service from the point of disruption to the point when the specific business service is recovered to a level sufficient to meet business obligations.

Dependency Mapping

Given the interconnectedness of the financial sector, FIs should conduct Dependency Mapping[3] to identify and map the end-to-end dependencies covering people, processes, technology, and other resources that support each critical business service. This will allow the FI to better understand the implications of the unavailability of these resources and come up with a plan to ensure its business functions and dependencies can meet the SRTOs during a crisis.

For Third-Party[4] dependencies, FIs may adopt the following non-exhaustive measures to ensure its Third Parties are able to meet the SRTOs of its critical business services.

- Establish and regularly review operational level or service level agreements with Third Parties that set out specific and measurable recovery expectations and support the FI's BCM.
- Review the BCPs of Third Parties and verify that the BCPs meet appropriate standards and are regularly tested.
- Establish arrangements with Third Parties to safeguard the availability of resources, such as requesting for dedicated manpower.
- Conduct audits on the Third Parties.
- Perform joint tests with Third Parties.

2. On-going Review and Risk Management Measures

Threat Monitoring, Review and Reporting

FIs should be cognizant of the evolving nature of possible threats and disruption and take steps to ensure its BCM preparedness remains an on-going effort. FIs should institute an escalation process to promptly alert internal stakeholders and senior management about such threats and identify areas of improvements/gaps following a crisis.

As part of its on-going efforts, FIs may consider utilising additional tools and automation that could enhance its BCM implementation (e.g., communication tool for activation and notification of personnel, situational dashboards that can provide real-time incident updates etc).

FIs should update its BCM policies and procedures upon any change of its operational environment and threat landscape, and review its critical business services and functions, its SRTOs/RTOs and dependencies **at least annually or whenever there are material changes.**

Concentration Risk Management

Concentration risk may arise when:

(i) people, technology, and other required resources are concentrated in the same zone; and/or

(ii) several of its critical business services/functions are outsourced to a single service provider.

[3] "Dependency Mapping" is a process to identify and understand the internal and external dependencies on people, processes, technology, and other resources (including those involving Third Parties) for each critical business service.

[4] "Third-Party" refers to external service providers, including intra-group service providers that support the delivery of the FIs' critical business services.

To mitigate the risk of concentration risk, FIs may consider adopting the following measures:

Examples of Concentration Risk Mitigants	What Needs to be Done
Establishing a primary-secondary site operation	Separate primary and secondary sites of critical business services and functions, or infrastructure (such as data centres) into different zones to mitigate wide-area disruption.
Ensuring critical business functions segregation	Separate critical business functions into different zones to mitigate the risk of losing multiple critical business functions, and the critical business services that they support, from a wide-area disruption.
Instituting split team and back-up team arrangements	Deploying critical personnel across different zones, or establish reserve team arrangements to eliminate the dependency on a single labour pool.
Ensuring cross-training of staff	Identify critical skills or roles, and develop cross-training programs to build versatility for key personnel involved in these roles.
Activating cross-border support	Activate cross-border support as a contingency during disruptions.
Engaging an alternative service provider	Engage an alternate service provider for redundancy, or to be activated to provide immediate support when the primary service provider is unavailable.

Regular Testing

FIs should conduct regular testing to validate its BCM preparedness. The frequency and scope of testing should be commensurate with the criticality of the FI's business services and functions, and should ideally meet the following test objectives:

Test Objectives
✓ Validate and measure the effectiveness of the BCPs using appropriate metrics ✓ Remediate any gaps or weaknesses that are identified in the recovery process ✓ Familiarise personnel in business continuity and crisis management with their roles and responsibilities ✓ Sensitise senior management and staff involved to the potential areas of concern that could arise in crisis situations, and practise making decisions under simulated conditions ✓ Stress test BCPs under severe but plausible scenarios ✓ Verify that the SRTOs of its critical business services and RTOs of its critical business functions can be met through the established recovery strategies.

FIs should ensure that all test records are properly documented and the following details are captured.

- Test objectives
- Scope
- Scenario design
- Participants involved
- Results
- Follow-ups for each test

Any gaps and weaknesses identified should be promptly reported to senior management and any remedial actions taken should be followed up with. FIs are also encouraged to participate in joint-response industry exercises.

3. Crisis Handling

Incident Management

FIs should have in place, robust processes to manage incidents to resume critical business services and functions within the stipulated SRTO and Recovery Time Objectives ("RTO").

Crisis Management

Senior management is responsible for overseeing the FI's crisis management activities and for steering it out of a crisis. FIs should have the following non-exhaustive action plan to be better prepared in times of crisis.

- A crisis management structure, with clearly defined roles, responsibilities, reporting lines, and chain of command.
- A set of pre-defined triggers and criteria for timely activation of the crisis management structure.
- Plans and procedures to guide the FI on the course of actions and decisions to be made during a crisis.
- Tools and processes to facilitate timely updating and assessment of the latest situation to support decision-making during a crisis.
- A list of all internal and external stakeholders to be informed when a critical business service is disrupted, as well as communications plans and requirements for each stakeholder.
- 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.

Communication with Staff

FIs are responsible for ensuring they have proper channels in place to communicate and update staff on developments during an incident or crisis and should provide crisis counselling support to staff who may suffer from crisis-induced psychological trauma.

Communication with External Stakeholders

FIs should ensure that it provides proactive, factual, and transparent information to external stakeholders during a crisis. FIs should also:

(i) appoint a designated spokesperson responsible for addressing the media and public;
(ii) prepare a communications plan, drawer media statements to cater to different scenarios, and holding statements that can be released immediately in the event of a crisis; and

(iii) inform MAS of the disruption via the FI’s respective MAS review officers or the 24-hour MAS BCM Hotline (Tel: **6229 9526/ 6229 9527**), no later than one hour upon the discovery of incidents where business operations will be **severely disrupted or when the BCP is going to be activated in response to an incident.**

4. Governance

Audit

FIs should ensure that their BCM framework, including each of its critical business services, is audited at least **once every three years** by a qualified and independent party. Particular attention should be paid to:

- higher risk areas as identified from the FI’s risk assessment;
- previous audit findings; and
- relevant incidents.

FIs should have a process in place to track and monitor the implementation of sustainable remedial actions in response to the audit findings and escalate any significant audit findings that may have severe impact on the FI’s BCM to its Board and Senior Management.

Responsibilities of the Board and Senior Management

The MAS reminds FIs that their Board and Senior Management (“BSM”) are ultimately responsible for the FIs’ BCM and places such emphasis on the oversight and respective supervisory duties of the BSMs, as set out in the table below.

Roles and Responsibilities	
Board	**Senior Management**
The Board, or the committee delegated by it, should ensure that: (a) an effective and comprehensive BCM framework is established and maintained to manage potential operational disruptions, and to meet its business needs and obligations; (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; (d) the effectiveness of the BCM framework is regularly reviewed and evaluated against external events, changes in risk profiles and business	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, their

priorities, or new processes, systems, or products or services; and (e) an independent audit is performed to assess the effectiveness of controls, risk management and governance of business continuity preparedness of the FI.	SRTOs and RTOs are commensurate with its business needs and obligations; (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 and functions are able to recover within their SRTOs and RTOs; (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) 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. Note: 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 that require the Board's attention.