Guidelines on Business Continuity Management

June 2022

Monetary Authority of Singapore

Contents

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 process transactions. Operational disruptions, if not recovered speedily, may compromise the ability of financial institutions ("FIs") to meet their business obligations, resulting in financial and reputational damage, as well as inconvenience to customers. Given that FIs are highly interconnected, severe disruptions may have a broader contagion effect on the financial system.

1.2 MAS is concerned with both the soundness of individual FIs and the stability of the financial system. FIs are thus expected to have controls in place to minimise the occurrence of operational disruptions, including the identification of potential single points of failure early on and their elimination, where possible.

1.3 Despite an FI's best efforts to achieve operational resilience, disruptions could still occur due to various factors, some of which may not be within its control. An effective Business Continuity Management (BCM) framework is therefore critical in minimising the impact of any operational disruptions on an FI's ability to continually deliver financial services.

Application of Guidelines

1.4 This set of MAS Guidelines on BCM (hereafter referred as "the Guidelines") contains sound BCM principles that FIs are encouraged to adopt. FIs are ultimately responsible for their business continuity preparedness and recovery from operational disruptions. FIs should establish policies, plans and procedures to ensure that their critical business services and functions can be promptly resumed following a disruption.

1.5 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.

1.6 As part of its supervision, MAS will review the BCM of an FI, taking into account the extent to which the Guidelines have been observed, to assess the quality of its oversight and governance structure, internal controls, and risk management. Particular attention will be accorded to the BCM of an FI's critical business services.

1.7 FIs' senior management and personnel, who are responsible for implementing BCM, should familiarise themselves with the Guidelines and understand their intent and implications. 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.

1.8 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.

1.9 This set of Guidelines is applicable to all FIs as defined in Section 2 of the Financial Services and Markets Act 2022.

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.
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 the FI.
Critical Business Function	A business function which, if disrupted, is likely to have a significant impact on the 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, its customers or other FIs that depend on the business service.
Dependency Mapping	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.
Recovery Time Objective (RTO)	Target duration of time to restore a specific *business function* from the point of disruption to the point when the specific *business function* is recovered to a level sufficient to meet business obligations.
Service Recovery Time Objective (SRTO)	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[1] sufficient to meet business obligations.
Recovery Strategy	A defined, management-approved and tested course of action by the FI to ensure the recovery and continuity of business services and functions in the event of operational disruptions.

[1] 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.

2 Critical Business Services and Functions

2.1 Business functions underpin the provision of business services to an FI's customers. When 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. There may also be some business functions that do not directly contribute to business services[2], but their disruption could impact an FI's safety and soundness.

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. The FI should therefore prioritise the recovery of its business services and functions based on their criticality, and determine the appropriate recovery strategies and resource allocation.

2.3 The FI should identify[3] its critical business services (refer to **Appendix: Examples of Business Services**) and functions by considering the impact of their unavailability on:

(a) the FI's safety and soundness[4];

(b) the FI's customers, based on the number and profile[5] of customers affected, as well as how they are impacted; and

(c) other FIs that depend on the business service.

2.4 In establishing recovery strategies, the FI 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 the FI.

[2] Examples of such business functions may include payroll processing, security operations centre, legal and compliance.

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

[4] This include assessing the extent of damage to the FI's financial and liquidity position, any loss of assets and revenue, loss of business and investments, and any inability to meet legal and regulatory obligations (including sanctions compliance).

[5] This should take into consideration the type of customers (e.g. retail/corporate/interbank customers).

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

3 Service Recovery Time Objective

3.1 The FI should establish a **Service Recovery Time Objective (SRTO)** for each critical business service. The SRTO, being a time-based metric, provides clarity within the FI on the expected recovery timelines for each business service. This will help to guide the prioritisation of resources during planning, and facilitate decision-making and monitoring of the recovery progress in a disruption.

3.2 In establishing SRTOs, the FI should take into consideration its obligations to customers, as well as other FIs that depend on the business services. The FI is expected to put in place recovery strategies[6] to enable it to achieve the established SRTOs and recover to the service levels required to meet its business obligations. For critical business services that are supported by a number of business functions, the FI must ensure that the Recovery Time Objectives (RTOs) of the underlying business functions and their dependencies will meet the SRTOs.

3.3 The FI should also set out clearly defined criteria for BCP activation when a critical business service encounters partial disruption (including intermittent or reduced performance that is not tantamount to a complete unavailability of service). This will guide the FI in activating its BCP in a timely and decisive manner, before the service degradation worsens to the point that it results in severe impact.

[6] 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 Dependency Mapping

People, Processes, Technology and Other Resources

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 these linkages, the FI should identify and map the end-to-end dependencies covering people, processes, technology and other resources[7] (including those involving third parties) that support each critical business service.

4.2 The dependency mapping will enable the FI 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. The FI should use the information derived from the dependency map to verify that the recovery of the business functions and their dependencies can meet the established SRTOs.

Third-Party Dependencies

4.3 Many FIs engage third parties[8] 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 put in place measures that enable third parties to meet the SRTOs of its critical business services. This can be done through measures, such as the following:

(a) 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;

(b) review the BCPs of third parties and verify that the BCPs meet appropriate standards and are regularly tested;

(c) establish arrangements with third parties to safeguard the availability of resources, such as requesting for dedicated manpower;

[7] Other resources include data in both digital and non-digital form.

[8] These will include intra-group service providers.

(d) conduct audits[9] on the third parties; or

(e) perform joint tests with third parties.

4.5 The FI should also put in place plans and procedures[10] to address any unforeseen disruption, failure or termination of third-party arrangements to minimise the impact of such adverse events on the continuity of its critical business services.

4.6 As far as possible, the FI should put in place measures to address the disruption of common utility services [11] supporting critical business services, such as implementing redundancy or alternative contingency arrangements.

[9] Audits performed as part of a certification process (e.g. ISO 22301 Security and Resilience – Business Continuity Management Systems) 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.

[10] 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.

[11] Examples include telecommunications networks and power utilities.

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 zone[12]. FIs may also be exposed to concentration risk when several of its critical business services and/or functions are outsourced to a single service provider. As skilled people, information, and systems are important assets that are difficult to replace quickly, FIs will need to adopt sound and responsive risk management to address concentration risk.

5.2 The FI could consider adopting the following approaches to mitigate the risk of concentration and reduce the impact in the event of a disruption:

(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;

(b) 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;

(c) split team and back-up team arrangements – deploying critical personnel across different zones, or establish reserve team arrangements[13] 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;

[12] A zone refers to an area or region that shares a similar risk profile such that people, data, systems, and other key resources located in the same zone would likely be affected by a disruption. 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 criterion that defines a zone that could be applied equally across the financial sector.

[13] 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.

(e) cross-border support – activate cross-border support as a contingency during disruptions[14]; or

(f) 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.

5.3 Taking into consideration learnings from pandemics (e.g. SARS, H1N1, COVID-19), the FI should be cognizant 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 challenges[15]. The FI should also put in place mitigating controls[16] to address such new risks and challenges.

[14] Cross-border support may subject an FI 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.

[15] 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.

[16] 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 BCM is an ongoing effort to ensure that the measures put in place are able to address operational risks posed by the latest threats, as well as plausible threats in the future. The FI should adopt a proactive business continuity posture by embedding BCM into its business-as-usual operations and establish BCPs that address a range of severe and plausible disruption scenarios, which may evolve over time.

6.2 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. The FI should proactively address such risks, and continuously seek out areas to enhance and ensure that its BCM remain relevant and forward looking. This will strengthen the FI's abilities to manage any unforeseen disruption to its business services.

Threat Monitoring, Review and Reporting

6.3 The FI should actively monitor and identify external threats and developments that could disrupt its normal operation, and have an escalation process to alert internal stakeholders and senior management about the relevant threats in a timely manner.

6.4 The FI 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 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

6.5 The FI should perform a review to identify areas of improvement and address any gaps in its BCM measures following an operational disruption. The FI should also draw lessons learnt from its own near misses, as well as incidents in other organisations, to enhance its business continuity preparedness.

6.6 The 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 tools that enhance the FI's BCM implementation or crisis management, such as automated workflows, templates and checklists, communications tool for activation and notification of personnel, as well as situational dashboards providing real-time updates on the incident.

6.7 The FI should update its BCM policies, plans, and procedures, including relevant training programmes for staff and test plans, based on changes in its operational environment

and the threat landscape. The FI should also review its critical business services and functions, their respective SRTOs/ RTOs and dependencies at least annually, or whenever there are material changes that affect them.

7 Testing

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

7.2 The FI should plan its test activities to meaningfully test all aspects of its BCM framework, and to meet the following test 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, including those of relevant third parties, involved in business continuity and crisis management with their roles and responsibilities. This includes how the alternate sites and recovery arrangements should be operated, so as to improve coordination and ensure a seamless execution of various plans;

(c) sensitise senior management and staff involved in crisis management 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 and functions;

(d) stress test BCPs under severe but plausible scenarios to allow the FI to challenge its current planning assumptions and ensure the relevance and effectiveness of its BCPs, to better mitigate the impact of severe disruptions; and

(e) verify that the SRTOs of its critical business services and RTOs of its critical business functions can be met through the established recovery strategies.

7.3 The FI should select the types of tests[17] that best meet these objectives, and set out the frequency and scope[18] of these tests to be commensurate with the criticality of the business services and functions. The 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. Gaps and weaknesses identified from the FI's business continuity testing should be reported to the senior management.

Remedial actions

7.4 Being able to clearly track and assign ownership of remedial actions is essential in ensuring that lessons learnt are systematically captured and used to improve the existing recovery processes. The FI 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 exercises[19] organised by government agencies, regulatory bodies, industry associations, and financial market infrastructure operators. Doing so would strengthen the joint response and coordination between institutions and improve the effectiveness in the financial sector's overall business continuity capability.

7.6 These exercises provide opportunities for the participating institutions to evaluate and discuss the impact of the FIs' actions on their external dependencies and the broader implications on the financial sector. This will allow FIs to gain useful insights to improve their BCM policies, plans and procedures.

[17] Types of tests could range from basic call-tree activation, crisis management exercises, business process recovery tests, data restoration testing, and cover scenarios such as alternate data centre or alternate site activation, operating with reduced headcount, operating in the absence of a key third party, relying on onsite generators for a prolonged period, etc.

[18] 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 and functions, 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.

[19] 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 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. The 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 FI should audit its overall BCM framework and the BCM of each of its critical business services at least once every three years. The audit should assess the adequacy and effectiveness of the FI's BCM. The audit should pay particular attention to higher risk areas identified from the FI's risk assessment, previous audit findings, and relevant incidents.

8.3 The BCM audits should be conducted by a qualified party who possesses the requisite BCM knowledge and expertise to perform the audit, and is independent of the unit or function responsible for the BCM of the FI.

8.4 The FI should establish processes to track and monitor the implementation of sustainable remedial actions in response to the audit findings. The FI 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.

9 Incident and Crisis Management

Incident Management

9.1 The FI should have robust processes to manage incidents in order to resume critical business services and functions within the stipulated SRTOs/RTOs. Where the delivery of a business service depends on multiple business functions, an overall coordinator should be appointed to coordinate incident management and recovery across affected functions.

Crisis Management

9.2 The FI's 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 procedures 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, as well as communications plans and requirements (i.e. drawer plans, 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

9.3 The FI should have in place channels to update staff on developments during an incident or a crisis. This includes 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

9.4 The FI should ensure that communications to its external stakeholders[20] are proactive, transparent, and factual. This will reassure stakeholders and maintain customer confidence during a disruption or crisis.

9.5 To facilitate timely public communications, the FI should have a communications plan and prepare drawer media statements that cater to different scenarios and holding statements that can be released immediately in the event of a disruption. Where necessary, the FI 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 spokesperson(s) who will be responsible to address the media and the public.

9.6 The FI should ensure that MAS is notified as soon as possible, but not later than one hour[21] 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. In the notification, the FI should provide information as per the MAS incident reporting template, 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.).

[20] External stakeholders include customers, media, government authorities and regulators, etc.

[21] FIs should notify MAS through their review officers or the MAS BCM Hotline. The instructions on incident notification and reporting to MAS, and the incident reporting template can be downloaded from the MAS website.

10 Responsibilities of Board and Senior Management

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 and functions 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 the leadership and strategic direction to 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 Board[22] and senior management should build an organisational culture that has business continuity preparedness embedded within the FI's day-to-day risk management[23], 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, 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;

[22] 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.

[23] 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 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

(e) 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, their 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.

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. The attestation should also be provided to MAS upon request.

Appendix: Examples of Business Services

Types of Business Services	Examples of Business Services[24]
Banking	Cash transactions Lending Deposit-taking Treasury[25] 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

[24] Business services are external-facing services that are provided to customers of an FI. These examples listed in the Appendix are non-exhaustive. FIs should identify the business services that are critical depending on the nature, size, and complexity of its business operations.

[25] This refers to the provision of external-facing Treasury services to customers (e.g. institutional sales).


MAS
Monetary Authority of Singapore