waystone | Compliance Solutions

BCM – MAS Guidelines

Introduction

On 6 June 2022, The Monetary Authority of Singapore (MAS) released the revised Business Continuity Management Guidelines (BCM Guidelines). BCM Guidelines are applicable to all financial institutions (FIs) and emphasise the need for all FIs to maintain their business continuity and resilience against disruptive events such as cyber-attacks and pandemic outbreaks. The extent and degree to which an FI implements the BCM Guidelines should be commensurate with the nature, size, risk profile and complexity of its business operations.

Effective business continuity management procedures are essential for efficient and safe continuation of business in today's world. MAS has indicated that as part of its supervision, FIs will be assessed on how well they have adopted the BCM guidelines within their organisation and particular attention will be placed on business continuity management of an FI's critical business services.

Key points:

1. The Guidelines set out the need for financial institutions to take an end-to-end (both business flow and internal flow) service-centric view in ensuring the continuous delivery of critical business services to their customers.
2. Although customers are the primary objective to be protected, it should be noted employees and the market itself are also protected.
3. The new guidelines require FIs to go further, much further than before, adopt a service centric approach, it demands that the customer is the focal point of all decisions in respect of When Bad Happens or could Happen!

   Key Message: New principles and practices that firms must implement to strengthen their operational resilience.

Identification/ Mapping	— Identify those critical business services, map end to end dependencies, unique to your firm. — In addition to critical business functions, the firms are to safeguard the delivery of services to customers, on an ongoing basis (covering people, processes, technology, and other resources). — Customers must have confidence if an event occurs the firm has resilience built into their plans.
Assessment	— Financial institutions must assess the critical Business Services, external facing service, which if disrupted on short term or long term, is likely to have a significant impact on the firms' safety and soundness, its customers or other firms that depend on the business service. — Must undertake robust assessments, Critical Business Functions, which is an activity performed by individual organisational lines, like department or unit, which, if disrupted, is likely to have a significant impact on the firms, whether directly or indirectly, financially, or non-financially.
Recovery Times	— Firms must set target recovery times and establish Service Recovery Times, with the objectives to provide clarity on the recovery expectations for critical business services (e.g., if insurance broker would be claims servicing, policy renewal and servicing, Policy inception).
BCM Audit	— Firms must conduct a BCM audit, the audit to cover the firms overall BCM framework and the BCM of each of its critical business services, on the adequacy and effectiveness of its BCM framework, at least once every three years.
Governance & Internal Controls	— The Board and senior management are ultimately responsible for the firm's BCM, they MUST have (a) crisis management structure, plans and procedures (b) conduct regular and comprehensive testing (c) validate the effectiveness of response and recovery arrangements (d) remediate any gaps or weaknesses identified (e) mitigate concentration risk.

What is Business Continuity Management?

Business continuity management (BCM) is a holistic management process that identifies potential impacts that threatens an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of stake holders, clients, and reputation of the organisation.

BCM is a management led process which identifies and mitigates risk and disruptions that could affect the capability of the organisation to continue to deliver its prioritised activities during a disruptive incident.

BCM is established for the overall identification of potential events, the likelihood of the occurrence of these events and the predicted impact to the organisation. BCM is more focused on the continuation of the whole business in the face of any unforeseen events. Disaster recovery is viewed as more of a plan, with a supporting infrastructure, which is enacted in the event of a disaster.

Primary Objective: Mitigate risks posed to your firm by identifying your critical operations and applying a methodical approach to the threats that are posed to them.

Firms should consider the seven '**P**'s when developing their plan to keep the business operational:

Providers (internal and suppliers),

Performance (service level agreements you need to meet),

Processes,

People,

Premises,

Profile (your brand),

Preparation.

Your firm needs to ensure plans are communicated, understood, and made available to key staff, employee awareness is important. Balancing what is included and not, is of vital importance, share non-confidential aspects with clients and other key stakeholders which can assist with confidence in your firm's ability to maintain 'business as usual'.

Your documented plan should be a living document and not just sit in a folder or shelf!

BCM should not been seen as a tick box exercise, as it can add real benefit to the business by capturing key information in one document and assessment of the firms' activities.

Why have a BCM?

Excluding the regulatory clear obligation to have a BCM, it does make good business sense as well:

- Establish adequate levels of prevention and resilience in the firms' services to mitigate impact of a potential disaster or other disruptions to normal business operations (e.g., detailing actions to be taken to keep the firm in business).
- Protect and support the firms' employees, assets in the event of disruption and resume critical activities.
- Define, priorities, support critical functions in a pre-defined time-period (with output documented in this business continuity plan).
- Resume normal activities including information technology infrastructure and operations, within the best possible timeframe to meet the recovery time objectives and service recovery time objectives. In an emergency, it is important to remember that human safety is always the highest priority.
- Impart awareness of business continuity plan to all employees and, where applicable, to relevant third parties.
- Ensure necessary arrangements are in place to support critical services in the event of a disruption with third-party service providers, vendors, and suppliers.
- Minimize impact of a business disruption in the event of a major incident.

Know Your Company?

Before you can begin to design your business continuity plans or review them, you need to be able to define your company.

For example:

1. A company is not just defined by what its output is, but also by what shapes and influences it.

   There may be stakeholders and regulations that have a say in what matters to your company. They might influence your planning.

   a. List the internal and external issues that drive the need for business continuity planning.
   b. List your stakeholders and their requirements.
   c. List relevant laws and regulations and have a process for this.

2. Limit your Business Continuity Management System (BCMS) to what really matters.

   By knowing your companies and armed with your mission or business goals, you can set a boundary to your Business Continuity Management System (BCMS).

   You probably don't need a plan for the entire company; constrain the scope to the things that matter.

   a. List what parts of the organization that should be in the scope.
   b. List the outputs (Products and Services) that should be in the scope.
   c. Document and explain the exclusions.

3. Make sure your top management is committed to business continuity.
   Just as senior leaders direct and resource a company so it fulfils its purpose, they must do the same for business continuity management.

   It starts with a policy that is a statement of intent, which in turn drives the need, the activities, and the resources.

   a. Write a Business Continuity Policy.
   b. Disseminate the policy to everyone affected by it (both internal and external).
   c. Define roles and responsibilities for business continuity.
   d. Make sure someone from your senior leadership is responsible for the BCMS and document what their responsibilities are.

Unexpected disruption can have a huge cost to business, so insure your organization against worst case scenarios with a robust BCM, as well as consider if other protection such as insurance coverage can assist you.

What are Critical Business Services and Functions?

Firms are required to comply with MAS TCA-No5: Notice on Technology Risk Management as per the Technology Risk Management regulations.

This Notice sets out:

1. MAS defines “critical system” in relation to a trust company, means a system, the failure of which will cause significant disruption to the operations of the trust company or materially impact the trust company’s service to its protected parties, such as a system which— (a) processes transactions that are time critical; or (b) provides essential services to protected parties.
2. Prior to implementation of any new services, systems or hardware, the firm performs an assessment to identify if the system being installed would be defined as a critical application.

Most areas of a business are essential to its overall functioning and operation. However, some are critical and must be afforded priority in terms of resources, space, and time in the event of an emergency. These functions and processes are deemed as “critical business services and functions” and must be operational within the shortest time possible, as disruption could impact the firm’s safety and soundness.

Without such critical business services and functions (i.e., technology, operational or supportive), the firm] would be unable to achieve its objectives or meet regulatory and/or legal requirements. Critical business functions include functions that do not directly support any critical business services but may still impact the firm significantly when they are disrupted.

Critical business services and functions includes:

- Payroll processing;
- Security operations center;
- Legal and compliance;
- External facing services such as portfolio management, trustee services, fund administration, valuation, processing of subscriptions and redemptions, cross border payment transactions.

The firm must conduct assessments to identify critical business services and functions. In conducting the assessment, the firm identifies business services and functions that if unavailable, could pose a risk to the firm’s safety and soundness, or adversely impact its customers and other financial institutions.

The following guidelines are used to assess impact of critical business services and functions to firms:

FI’s Safety and Soundness	— Damage to FI’s financial and liquidity position — Loss of assets and revenue — Loss of business and investments — Inability to meet legal and regulatory obligations
FI’s customers	Potential impact of customers based on: — Number of customers — Type of customers (retail, corporate, institutions) — How customers will be impacted when business / function is unavailable
Are other FI’s dependent on the business service	— Extent of systemic impact on financial sector

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

It should be noted firms have a regulatory obligation to put in place a framework and process to identify critical systems and make all reasonable efforts to maintain high availability of these systems of the firm, shall ensure that the minimum unscheduled downtime for each critical system that affects the operations or service to customers do not exceed a total of 4 hours within any 12-month period. Firms must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system and validate and document how it performs its system recovery testing and whether RTO is validated during the system recovery test, at least once every 12 months.

Upon discovery of a relevant incident, firms must inform MAS within 1 hour. A root cause and impact analysis report must also be submitted to MAS within 14 days should such a relevant incident be discovered.

BCM Testing

Testing of the BCM is a vital step, the actual test is for your firm to consider and undertake linked to your operations, to decide the scale/objectives for this as the regulated entity.

The development of testing strategies requires a business decision regarding the level and frequency of testing needed to ensure recovery objectives can be achieved during a business interruption or disaster.

The frequency and complexity of testing is based on the risks to the institution. Even small, serviced institutions should participate in tests with their core service providers and test other critical components of the BCP.

Testing strategies should detail the conditions and frequency for testing applications and business functions, including the supporting information processing. The strategy should include test objectives, scripts, and schedules, as well as provide for review and reporting of test results. Management should ensure recovery testing is conducted at least annually, or more frequently, depending on the operating environment and criticality of the applications and business functions.

Management should clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test. The objective of a testing program is to ensure that the BCP remains accurate, relevant, and operable under adverse conditions. Testing should include applications and business functions that were identified during the impact analysis. The business impact analysis determines the recovery point objectives and recovery time objectives, which then help determine the appropriate recovery strategy.

Testing objectives should start small, and gradually increase in complexity and scope. The scope of individual tests can be continually expanded to eventually encompass enterprise-wide testing, including vendors and key market participants.

Achieving the following objectives provides progressive levels of assurance and confidence in the plan. At a minimum, a clearly stated testing plan should:

- not jeopardize normal business operations.
- gradually increase the complexity, level of participation, functions, and physical locations involved.
- demonstrate a variety of management and response proficiencies, under simulated crisis conditions, progressively involving more resources and participants.
- uncover inadequacies, so that configurations and procedures can be corrected; and
- consider deviating from the test.

A useful test can only be achieved if the test results are analysed and compared against stated objectives and acted upon.

Management should report the test results and the resolution of any problems to the board. Management reports should consider all the test results. Test analyses must include:

- an assessment of whether the test objectives were completed;
- an assessment of the validity of test data processed;
- corrective action plans to address problems encountered;
- a description of any gaps between the BCP and actual test results;
- proposed modifications to the BCP; and
- recommendations for future tests.

These tests should determine the quality and effectiveness of the organisation's business continuity planning process. These procedures will disclose the adequacy of the planning process for the organisation to maintain, resume, and recover operations after disruptions ranging from minor outages to full-scale disasters.

Your firm needs to consider the BCP plan and test activities to meaningfully way, test all aspects of its BCM framework, and to meet the defined test objectives, such as:

1. Validate and measure the effectiveness of the BCPs using appropriate metrics, and remediate any gaps or weaknesses that are identified in the recovery process;
2. 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 must be operated, to improve coordination and ensure a seamless execution of various plans;
3. 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;
4. stress test BCPs under severe but plausible scenarios to allow your firm to challenge its current planning assumptions and ensure the relevance and effectiveness of its BCPs, to better mitigate the impact of severe disruptions; and

Your firm should vary the types of tests to ensure its plans are fully tested, these could range from basic call-tree activation, crisis management exercises, business process recovery tests, data restoration testing, retrieval of vital records and cover scenarios such as alternate data center 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.

Exercise Examples:

- Direct Desktop Check: For this you can go through your plans against known requirements/ operations and write a report with improvement actions.
- Walk Through: Physically walk through the processes and procedures recorded in the plan, and then mitigate to fix any errors identified.

  (Note – 50-60% of exercises should be one of the above)
- Call Tree: Send out a test message to ensure your staff will receive your communications.
- Simulation: Select an incident type, pose it, and ask for a theoretical response.
- Limited rehearsal: Ask a specific business unit to respond to an incident.
- Full exercise: put into place the organizations complete business continuity arrangements.

Dependency Mapping

Dependency mapping is the 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.

People, Processes, Technology and Other Resources

Financial institutions have become increasingly interconnected with the growing reliance on common IT systems and third parties. As a primary first step to mitigate the risks arising from these linkages, firms must identify and map the end-to-end dependencies covering people, processes, technology, and other resources (including those involving third parties, data in both digital and non-digital form) that support each critical business service.

The objective of the dependency mapping will enable the firm 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. Firms must 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.

Definition	Explanation	Category
Mapping	Identifying, documenting, and understanding the chain of activities involved in delivering critical or important business services. 1. Do not map all processes at once or map the process at a detailed level. 2. Start by identifying and agreeing upon the critical processes, assign ownership and begin by mapping these processes according to a predefined template.	Operational Resilience Technology
Processes and Resources	This includes the processes and their relationship with key resources: a. people b. technology c. facilities d. information	Operational Resilience
Inter-dependencies	These are the internal and external dependencies on people, processes, technology, and other resources (including those involving third parties) for each important or critical business service.	Operational Resilience
Inter-connections	These are the linking of an organisation's network with products, services, equipment, or facilities not belonging to the originating organisation's network. The term may refer to a connection between the organisation's facilities and the equipment belonging to its customer, or to a connection between two or more parties.	Operational Resilience

Linking to Outsourcing requirements, identify your 'critical' suppliers and ensure they have business continuity arrangements in place that fit with your objectives and are defined within your contract. Also consider setting up more than one source of supply or increasing your stock of critical resources.

Firms in Singapore have established that there are economic benefits to be gained through the centralisation of operations, however, those firms need to be fully aware that concentration risk may arise when there is concentration of people, technology, or other required resources in the same zone.

As a result, firms 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, the firm must adopt sound and responsive risk management to address concentration risk.

BCM Audit

Firms must conduct an independent audit on their BCM preparedness at least once every three years. This needs to be performed by a qualified party who is independent of the unit or function responsible for the BCM of the firm.

Firm must ensure that their audit programme adequately covers the assessment of BCM preparedness based on the level of operational risks that we are exposed to.

Firms are required to:

1. Audit your overall BCM framework and the BCM of each of its critical business services at least once every three years. This audit must assess the adequacy and effectiveness of the firm's BCM. The audit must pay particular attention to higher risk areas identified from the firm's risk assessment, previous audit findings, and relevant incidents.
2. Appoint a qualified party (either internal audit qualified person) or external service provider such as Waystone) to conduct the audit, 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 firm.
3. Establish processes to track and monitor the implementation of sustainable remedial actions in response to the audit findings. Firm's must escalate any significant audit findings on lapses that may have severe impact on our BCM to the Board and senior management.
4. Submit the BCM audit reports to MAS upon request.

Example Audit Questions:

1. Does the FI understand and regularly monitor the expectations of interested parties, such as customers, suppliers, employees, or regulatory bodies, in Its business continuity plan?
2. Has the FI conducted a gap analysis of your existing BCM framework and policies against the 2022 BCM Guidelines, and documenting this gap analysis?
3. Does the FI provide strong governance over BCM and can evidence it?
4. Have recovery priorities and timescales been agreed for mission-critical services and processes?
5. Has the FI's undertaken an assessment to Identify and map end to end dependencies?
6. Has Dependency mapping been fully completed and documented?
7. Does the FI prepare after-action reports to detail what went well and what didn't go well in business continuity system exercises?
8. Have all staff been made aware of your business continuity arrangements?
9. Are SRTOS, RTOs and dependencies annually or upon material changes?
10. Have clear procedures been developed for making sure that changes in the business are reflected in the Plan (personnel, processes, resource requirements, etc)?
11. Have the policy and objectives for the BCM, which should be compatible with the context and strategic direction of the organization, been established and communicated?

Record Keeping

Over time, records can become outdated and insufficient representation of current plans, procedures, records, etc is possible.

It is essential that records are updated appropriately following a predetermined schedule.

If vital records are not updated and thusly destroyed, incomplete or inaccurate information may be relied upon during emergencies and outdated information and records can slow the continuation and reconstitution of essential functions.

Ensure your plan is well documented and easily accessible, your firm should work with the key stakeholders (including suppliers) to put in place 'back to normal' recovery plans and ensure they are agreed and documented.

Top Tips:

- FIs must take a step back, identify those critical business services, unique to the FIs, but in addition to critical business functions, the FIs must safeguard the delivery of services to customers, on an ongoing basis and customers must have confidence that if an event occurs, the FIs have resilience built into their plans.
- FIs must assess the critical business services, external facing service, which, if disrupted on short term or long term, 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.
- FIs must undertake robust assessments of critical business functions, which is activity performed by individual organisational lines, such as department or unit, which, if disrupted, is likely to have a significant impact on the FI, whether directly or indirectly, financially, or non-financially.
- FIs must set target recovery times and establish service recovery times, with the objectives to provide clarity on the recovery expectations for critical business services.
- FIs must identify and map end-to-end dependencies, and through this it should cover people, processes, technology and other resources (including those involving third parties) that support each critical business service.
- Significantly, FIs must conduct a BCM audit, to cover the FI's overall BCM framework and the BCM of each of its critical business services, concentrating on the adequacy and effectiveness of its BCM framework, at least once every three years.
- FIs must continuously review and improve through proactively monitoring and scanning for relevant threats that could disrupt its normal operations and they must continually seek out areas to enhance and ensure that their BCM remains relevant and forward looking.
- FI's Board and Senior Management have full responsibility and the Board and Senior Management are ultimately responsible for the FI's BCM, they MUST (a) have in place crisis management structure, plans and procedures. (b) conduct regular and comprehensive testing (d) validate the effectiveness of the FI's response and recovery arrangements (d) remediate any gaps or weaknesses identified (e) mitigate concentration risk, by reducing exposure to risk arising from the concentration of people, technology, or other required resources in the same zone, or reliance on a single service provider.

How can Waystone help?

Waystone is a leading global provider of institutional governance, administration, risk, and compliance services to the asset management and financial services industry. Our global Compliance Solutions team helps clients navigate the regulatory landscape with confidence, aligning investment strategies and operational processes with compliance requirements. With over 100 compliance specialists based across Asia, the Middle East, Europe, and North America, we offer a comprehensive range of solutions, from company registration and licensing to compliance programmes and ongoing support.

In Singapore and Hong Kong, Waystone brings over 20 years of experience, working with clients regulated by the Monetary Authority of Singapore and the Securities and Futures Commission. Our team is well-equipped to provide bespoke, risk-focused, and cost-effective solutions. With extensive experience, we deliver the expertise you need while adding value to your corporate governance standards.

If you would like to discuss the themes raised in this guide with one of our APAC Compliance Solutions team members and learn how we can assist you, please contact us using the details below.

Contact Us →