مؤسسة النقد العربي السعودي

Saudi Arabian Monetary Authority

SAUDI ARABIAN MONETARY AUTHORITY (SAMA)

Business Continuity Management Framework

February 2017

Version 1.0

Table of contents

Introduction

1.1 Introduction to the BCM Framework

Considering the need of 24 x 7 availability of the business operations by financial institutions in the Kingdom of Saudi Arabia, SAMA has developed a Business Continuity Management (BCM) framework for member organizations that would enhance the organizational resilience capability to ensure continuity and availability of their operations and services. The requirements are based on SAMA requirements, industry practices and international standards, such as ISO 22301, ISO 27001, Good practice guidelines from BCI, and Professional practice guidelines from DRII. All Member Organizations are required to comply with these requirements and integrate it formally in their BCM program.

1.2 Definitions

- BCM is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
- BCM is part of the overall management system, which includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.
- IT Disaster recovery (IT DR) is part of BCM which includes policies, standards, procedures and processes pertaining to resilience, recovery or continuation of technology infrastructure supporting critical business processes.
- Maximum Acceptable Outage (MAO) is defined as the time that would take for adverse impacts which might arise because of not providing a product/service or performing an activity, to become unacceptable.
- Recovery Time Objective (RTO) is defined as the period following an incident within which, products or services must be resumed, activity must be resumed, or resources must be recovered.
- Recovery Point Objective (RPO) is defined as the point to which, information used by an activity must be restored to enable the activity to operate on resumption. This can also be termed as “Maximum Data Loss”.

1.3 Scope

The BCM framework document defines principles, objectives and control considerations for initiating, implementing, maintaining, monitoring and improving business continuity controls in member organizations.

The BCM framework document is applicable to the full scope of the Member Organization, including subsidiaries, employees, subcontractors, third-parties and customers.

The BCM framework document has an interrelationship with other corporate policies for related areas, such as enterprise risk management, health, safety and environment (HSE), physical security, cybersecurity (including cyber resilience and incident management).

1.4 Applicability

The BCM Framework document is applicable to following:

- All organizations affiliated with SAMA ("the Member Organizations")
- All banks operating in Saudi Arabia
- All banking subsidiaries of Saudi banks
- Subsidiaries of foreign banks situated in Saudi Arabia

1.5 Responsibilities

SAMA mandates the BCM framework requirements document to Member Organizations. This document outlines the BCM requirements to be implemented by the Member Organizations. SAMA is the owner and is responsible for periodically updating the BCM Framework document. The Member Organizations are responsible for adopting and implementing the requirements stated in this framework document.

1.6 Interpretation

SAMA, as the owner of the BCM framework requirements document, will provide interpretations of the principles, objectives and control considerations, if required.

1.7 Target Audience

This document is intended for board of directors, CEOs, chief risk officer, senior and executive management, business owners, owners of information assets, CIOs, CISOs, business continuity managers, internal auditors and for those, who are responsible for and involved in defining, implementing and reviewing business continuity controls.

1.8 Review, Changes and Maintenance

This document will be reviewed and maintained by SAMA. SAMA will review this document periodically to determine its effectiveness, including the effectiveness of the framework to address emerging business continuity threats and risks. If applicable, SAMA will update this document based on the outcome of the review.

If a Member Organization considers that an update to this document is required, the Member Organization should formally submit the requested update to SAMA after obtaining approval from the business continuity manager and business continuity steering committee within the Member Organization. SAMA will review the requested update, and when approved, this document will be updated.

Version control will be implemented for maintaining this document. Whenever any changes are made, the preceding version should be retired and the new version should be published and communicated to all Member Organizations.

1.9 Reading Guide

The BCM Framework represents the actual BCM domains and subdomains, principles, objectives, and control considerations.

2 Business Continuity Requirements

2.1 BCM Governance

Principle

The business continuity governance framework should be defined, approved, implemented and maintained, which should be monitored by senior management. The business continuity structure should be defined and communicated to all relevant employees and third parties.

Objective

To direct, control and evaluate the overall approach to business continuity within the Member Organization

Control Consideration:

1. Board of directors or a delegated executive member should have the ultimate responsibility for the BCM program.
2. The board of member organization, or a delegated member of senior management should allocate sufficient budget to execute the required BCM activities.
3. A BCM Committee should be established and mandated by the board of directors.
4. Senior management, such as CRO, COO, CIO, CISO, BCM manager and other relevant departments should be represented in the business continuity committee.
5. A business continuity committee charter should be developed and should reflect:
   a. Committee objectives
   b. Roles and responsibilities
   c. Minimum number of meeting participants
   d. Meeting frequency (minimum on quarterly basis)
6. A BCM function should be established.
7. A BCM manager/head should:
   a. Be appointed
   b. Have appropriate authority to manage the BCM program
   c. Be qualified and have appropriate experience, skills and competencies to implement and maintain the BCM program within the member organization
8. The BCM function should be adequately staffed with qualified team members
9. Cross-functional teams, consisting of strategic, tactical and operations team members should contribute in implementation and maintenance of the business continuity and disaster recovery plans.

2.2 BCM Strategy

Principle

A business continuity strategy should be defined and aligned with the Member Organization’s overall strategic business objectives.

Objective

To ensure that business continuity initiatives are in alignment with the strategic business objectives and embeds BCM as part of the good management practice within the Member Organization, in order to continual improvement in maturity.

Control Consideration

1. The business continuity strategy should be defined, approved, implemented and maintained.
2. The strategy should at minimum define:
   a. Long-term strategic objectives for implementing and maturing the BCM program
   b. Road map with timelines for achieving strategic objectives
   c. Requirements for continual review and validation of alignment of the BCM program with strategic objectives

2.3 Business Continuity Policy

Principle

A business continuity policy should be defined, approved and communicated to relevant stakeholders.

Objective

To document the Member Organization's commitment and objective of the business continuity program, and to communicate this to the relevant stakeholders.

Control considerations

1. A business continuity policy should be defined, approved, implemented and communicated
2. The business continuity policy should at the minimum identify:
   a. Objectives
   b. Scope
   c. Responsibilities
3. The compliance with the business continuity policy should be monitored .
4. The effectiveness of policy implementation should be measured and periodically evaluated.
5. Scope exclusions for the BCM should be documented and periodically evaluated. The justifications for scope exclusions should be documented and approved by BCM committee and senior management.

2.4 Business Impact Analysis (BIA) and Risk Assessment (RA)

Principle

The Member Organization should perform a business impact analysis and risk assessment for all relevant activities to determine the business continuity, and disaster recovery requirements and improvements.

Objective

To ensure that each Member Organization has identified and prioritized their business processes along with key dependencies, and identified adequate controls in order to fulfill their business, regulatory, legal and compliance requirements with regards to business continuity

Control considerations

1. Methodology for BIA and RA should be defined, approved, implemented and maintained.
2. The Member Organization should periodically perform a Business Continuity risk assessment. It should include, but not limited to:
   a. Identify potential internal and external threats, including single point of failures that may cause disruption to critical activities as determined in the BIA considering people, process, technology and premises
   b. Assess and prioritize potential risks by evaluating potential threats based on their operational impact and probability of occurrence
   c. Select required controls to manage identified risks
   d. Define treatment plan and implement BCM controls
3. The Member Organization should identify and prioritize the activities (i.e., products, services, business functions and processes) by performing BIA to determine the following but no limited to:
   a. The potential impact of business disruptions for each prioritized business function and processes, including but not restricted to financial, operational, customer, legal and regulatory impacts
   b. The recovery time objectives (RTOs), recovery point objectives (RPOs) and maximum Acceptable Outage (MAO)
   c. The internal and external interdependencies
   d. Supporting recovery resources
4. The BCM committee should endorse the prioritized list, BIA results, RA and the defined RTOs, RPOs and MAOs.
5. Risk assessment results should be communicated to the BCM committee
6. The BIA and RA should be updated annually and when major changes occur (such as change in structure and organization of people, process, technology, suppliers and locations).
7. The risk assessment should include risks associated with overall organization as well as data centers (primary and alternative), which are not owned by the Member Organization (e.g., consider the timeframe needed to relocate to a new site and accordingly, it should include a sufficient timeframe in the contractual agreement)
8. Capability of vendors, suppliers and service providers to support and maintain service levels for prioritized activities during disruptive incidents should be assessed at least on a yearly basis.
9. Member Organizations should ensure that RTOs are adequately defined for payment systems, customer related services, etc. considering the high availability of these operations and minimum disruption in the event of disaster.

2.5 Business Continuity Plan (BCP)

Principle

The Member Organization should define, approve and implement BCP for their critical activities. The compliance with BCP should be monitored, and the effectiveness should be measured and periodically evaluated.

Objective

To ensure that the Member Organization has the capability to identify and clearly define the actions to be taken, and resources which are needed to enable the organization in managing a disruptive interruption and to come back to a position where normal business processes can resume

Control considerations

1. A BCP should be defined, approved, implemented and maintained in readiness for use during disruptive incidents, to enable the Member organization to continue delivering its important and urgent activities, at an acceptable pre-defined level.
2. The member organization should define, approve and implement procedures for responding to disruptive incidents. The procedures should collectively include:
    a. Key resources (e.g., people, equipment, facilities, technologies)
    b. Defined roles, responsibilities and authorities for stakeholders
    c. A process to manage the immediate consequences of a disruptive incident and escalation procedures
    d. A process to continue the critical activities within predetermined recovery objectives (RTO, RPO and MAO)
    e. A process to resume the Member Organization's operations to business-as-usual once the incident is resolved
    f. Guidelines for communicating with employees, relevant third-parties and emergency contacts
    g. Process for including relevant cyber security requirements, if any, within the business continuity planning
3. The compliance with the BCP should be monitored.
4. The effectiveness of the BCPs should be measured and periodically evaluated.
5. The BCM Manager and BCM coordinators are responsible to maintain and keep the BCPs and arrangements up-to-date.
6. The Member Organization should have sufficient alternative business workspace(s) where it can relocate the required resources to deliver the critical processes required as per predefined recovery objectives in the BIA.
7. The alternative business workspace(s) should have clear demarcation of the sitting arrangement for different business units.
8. The Member Organization should implement sufficient logical, physical and environmental security controls in order to support the same level of access and security in case the alternative location needs to be activated.
10. For all critical activities, as determined by the BIA, the Member Organization should ensure that the key service providers (if any) have a BCP in place and their plans tested at least on a yearly basis.

2.6 IT Disaster Recovery Plan (DRP)

Principle

The Member Organization should define, approve, implement and maintain a IT DRP for its critical activities and related technology infrastructure.

Objective

To ensure the Member Organization has IT DRP and up-to-date list of critical activities in place, in case of a disruptive incident

Control considerations

1. An IT DRP to recover and restore technology services and infrastructure components (Data, systems, network, services and applications) should be defined, approved, implemented and maintained in alignment with business impact analysis.
2. The Member Organization should establish an alternative data center at an appropriate location. The location should be identified based on:
    a. A risk assessment to confirm that the location does not share the same risks of the main data center (e.g., geographical threat)
    b. Upon approval from SAMA
3. Data, system, network and application configurations, and capacities in the alternative data center should be commensurate to such configurations and capacities maintained in the main data center.
4. Member Organization should implement the same logical, physical, environmental and cyber security controls for the alternative data center as for the primary data center.
5. The Member Organization should define and implement a backup and recovery process.
6. The Member Organization should have offsite location for storing backups.
7. Formal contracts should be signed with third-parties to ensure the continuity of outsourced services or delivery of replacing hardware or software within the agreed timelines in case of a disaster. Include guidelines to ensure that the contracts signed with external service providers are aligned with the BIA and RA outcomes.
8. The IT manager should be responsible to maintain and keep the disaster recovery plans and arrangements up-to-date with an overall accountability of integration within the BCM Program on the BCM Manager.
9. The compliance with the disaster recovery plan should be monitored.
10. The effectiveness of the IT DRP should be measured and should be evaluated on a yearly basis as minimum.

2.7 Cyber Resilience

Principle

The Member Organization should ensure that critical services, business functions and processes run on reliable and robust infrastructure and software.

Objective

To ensure each that the Member Organization’s critical services, business functions and processes are available when required and resistant to disruptions.

Control considerations

1. All changes to the infrastructure and software, which directly support the identified critical services, business functions and processes, should:

   a. Be subject to in-depth risk assessments to ensure the agreed business requirements regarding availability and recovery are met.
   b. Follow strict development, testing and change management procedures to avoid single point of failures or malfunctioning.
2. A periodic architectural review should be defined and approved to ensure the business requirements regarding availability and business continuity are being correctly addressed and implemented.

   Note. For more control considerations to improve the overall resilience, e.g., threat management, vulnerability management, please refer to the SAMA - Cyber Security Framework.

2.8 Crisis Management Plan

Principle

The Member Organization should define, approve and implement a crisis management plan that would facilitate a well-managed response for major incidents, including rapid communication to ensure overall safety to both internal and external stakeholders.

Objective

To ensure the Member Organization has effective crisis management plan in place and up-to-date for critical member organization products, services, business functions and processes, in case of a disruptive incident.

Control considerations

1. A crisis management plan should be defined, approved and implemented.
2. The compliance with the crisis management plan should be monitored.
3. The effectiveness of the business continuity program within the crisis management plan should be measured and periodically evaluated.
4. The Member Organization should document a crisis management plan(s) that define(s) how crisis resulting from a major incident(s) will be addressed and managed, and should include at least:
   a. Criteria for declaring a crisis.
   b. The member organization should establish a command center for centralized management and an emergency command center.
   c. Crisis-management team members. Considering representatives of the critical products, services, functions and processes of the Member Organization (including Communications department)
   d. Contact details of those who are part of the crisis management team (including third-parties)
   e. Definition of the steps to be taken during and after a crisis or disaster (including the mandates required)
   f. Communication plan including the media response plan, to address the communication with the internal and external stakeholders during crisis.
   g. The frequency of crisis management tests

2.9 Testing

Principle

The Member Organization should define, approve, implement, execute and monitor regular BCP and DRP tests to train their employees and third-parties and test the effectiveness of the BC and DR plans.

Objective

To ensure that the Member Organization's existing BCP and DRP do work as defined and employees and third-parties are trained to execute these plans.

2.9.1 BCP testing

Control considerations

1. The Member Organization should periodically conduct BCP simulation test exercises ("at least once a year")
2. The tests should consider appropriate scenarios that are well planned with clearly defined objectives (e.g., per function, per service, per process, per location, per worst cases scenarios). The Member Organization should take into consideration to include cyber security scenarios.
3. Defined test scenarios should cover the activation and involvement for crisis management team.
4. After the completion of the above individual tests, each Member organization should consider conducting an integrated BCM test for all critical services, business processes and functions.

2.9.2 DRP testing

Control considerations

1. The Member Organization should periodically execute a DR test combined with BCP ("at least once a year").
2. The Member Organization should conduct an evaluation of the executed DR test of IT DR infrastructure that supports the Member Organization's critical systems to ensure the readiness and capability of DR to resume critical business operations for a period of time in case of a major disaster.
3. The DR test results should provide an evaluation and suggestions for improvements to manage disruptive events impacting the Member Organization's business continuity.
4. It should cover the activation and involvement of the crisis management team.

2.9.3 Executed tests

1. Detailed results of all exercises and tests should be documented for future reference. The exercises/tests results should include, but not be limited to the following considerations:
    a. Confirm meeting the objectives of the exercised plan
    b. Confirm capabilities and readiness of recovery resources
    c. Document lessons learnt and the required improvements
    d. In case of failure, Capture the root-cause of the failure and remediation actions should be tracked to successful conclusion

2. Re-testing of the plan within the defined timelines in case of a failure, the timelines should not exceed the limit of three (3) months.
3. The Internal Audit of the Member Organization, or a qualified external auditor, should observe the business continuity and disaster recovery testing activities as an independent participant in order to provide a reasonable assurance on the executed activities, test results and to observe if the executed tests are meeting the Member Organization’s overall Business Continuity program objectives.
4. All BCP and DRP tests results should be reported to the BCM committee, senior management and the board of directors.

2.10 Awareness and training

Principle
The Member Organization should establish, implement and maintain a training and awareness program that effectively supports the BCM objectives by developing the required competency among staff.

Objective
The Member Organization should ensure BCM integration into its day-to-day activities, through an ongoing awareness plan, which should be documented.

Control considerations

1. The Member Organization and relevant third-parties, such as providers and suppliers should be:
    a. Familiar with relevant parts of business continuity policy and plans
    b. Contractually bound to provide their services or products within the agreed time, in case of disruptive event
    c. Familiar with their point of contact or their local BCM coordinator in the Member Organization
    d. Familiar with their roles and responsibilities during disruptive incidents
2. A training program should be provided once on an annual basis to employees involved in BCM to achieve the required level of experience, skills and competences.
3. The Member Organization should periodically measure the effectiveness of the training and awareness program.

2.11 Communication

Principle
The Member Organization should define, establish and maintain a communication process for periodic communications with SAMA on matters related to its BCM program.

Objective
To ensure that continuous communication is maintained with SAMA by defining, agreeing and adhering to communication protocol, frequency, and roles and responsibilities for communications

Control considerations

1. The Member Organization should report all disruptive incidents classified as “Medium” or “High” to SAMA “Banking IT Risk Supervision” immediately. A post-incident report should be communicated to SAMA after the Member Organization resumes to normal operations.
2. The Member Organization should coordinate with SAMA Supervision when communicating with the media in case of incidents.
3. Member Organizations should seek SAMA’s approval when selecting a new site for its main or alternative data center, or when relocating the current main or alternative data center.
4. The Member Organization should communicate the approved program for executing business continuity and disaster recovery tests, for the upcoming year, with SAMA “Banking IT Risk Supervision” by end of January of every year.
5. Test results of business continuity and disaster recovery should be shared with SAMA within four weeks after the test. The Member Organization should identify the improvements based on the test performed and provide an action plan to SAMA within two months after the submission of the test results.

2.12 Periodic Documents Review

Principle

The business continuity and disaster recovery program, policies, plans and procedures should be reviewed and updated periodically, and in case of (major) change in the Member Organization’s critical products, services, business functions and/or processes.

Objective

To ensure that all the business continuity documents are up to date and can be used during a disruptive incident to recover the business operations.

Control considerations

1. Member Organizations should establish a process for document review/update to ensure the BC documents are up-to-date, reviewed and approved.
2. All documents should clearly identify the last date in which the document was reviewed and approved.

2.13 Assurance

Principle

The BCM of the Member Organizations should be subjected to periodically reviews and audits by a qualified independent internal or external party to ensure its effectiveness, and to obtain assurance regarding the compliance with the SAMA BCM.

Objective

To ensure that an independent party is reviewing the BCM framework activities and reporting the identified issues to the senior management independently.

Control considerations

1. Member organization should conduct review / audit of BCM by qualified independent internal/ external party.
2. the Member Organization should identify the gaps and provide a road map to enhance the BCM within the organization.
3. The identified gaps along with road map should be reported to senior management and BCM committee.