GUIDELINES ON BUSINESS CONTINUITY PLAN (BCP)

2022

Contents

Introduction 4

Preliminary 4

Objectives of Guidelines 4

Terms and Definitions 5

Critical Business Services and Functions 7

Risk assessment (RA) and Business Impact Analysis (BIA) 7

Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO) 8

Backup and recovery site 9

Dependency Mapping 10

People, Processes and Technology 10

Third-Party Dependencies 10

Continuous Review and Assessment 11

Threat Monitoring, Review and Reporting 11

Ongoing assessment 11

Exercising and Testing of BCP 12

Remedial actions 13

Audit 13

Incident and Crisis Management (Major Incident Handling and Escalation Strategy) 13

Incident Management 14

Crisis Management 14

Communications with Staff 14

Communications with External Stakeholders 14

Roles and Responsibilities of Board and Senior Management 15

Board of Directors 16

Senior Management 17

Appendix I: Critical Information Infrastructure for RA and BIA 19

Appendix II: Maximum Tolerable Period of Disruption (MTPD) 20

Appendix III: Example for the CII mapping for Financial Sectors 21

Annexure I. Incident Reporting Template 26

1. Introduction

Preliminary

1.1 The Guidelines on the Business Continuity Plan for all Financial Service Providers (hereafter referred to as FSPs is formulated and adopted as per Section 210 of the Financial Services Act of Bhutan 2011.

1.2 Trust and confidence in the financial ecosystem are the foundations for carrying out efficient operations such as financial transactions and safeguarding assets. If operational disruptions are not quickly resolved, financial service providers ("FSPs") capacity to fulfill their obligations may be jeopardized, resulting in loss of money, reputation and causing inconvenience to the customers. Given the interconnectivity of the FIs, major disruptions could have a broader ripple impact on the financial sectors.

1.2 RMA is concerned about the stability of the financial system as well as the soundness of individual FSPs. FSPs are therefore expected to have adequate safeguards in place to prevent and reduce the likelihood of operation disruptions, including the early intervention and elimination of potential single points of failure.

1.3 Disruptions may still occur despite FSPs' best efforts to build operational resilience for various reasons, some of which may be beyond its control. Therefore, it is essential to have an efficient Business Continuity Plan (BCP) structure to reduce the effect of any operational disruptions on an FSP’s capacity to continue providing efficient and effective financial services.

1.4 FSPs are required to maintain a copy of this plan both at the office and offsite. A copy of the plan will also be maintained offsite both electronically and in paper format. It is important to ensure that a copy of the plan is available to each team member, other staff and key emergency response partners for use in the event of a crisis. It is also important to ensure that the plan is kept up-to-date and that the team members have read the plan and understand its contents.

Objectives of Guidelines

1.4 This set of RMA BCP Guidelines (hereinafter "the Guidelines") offers basic BCP concepts that FSPs are mandated to implement. FSPs are accountable for their business continuity planning and recovery from any operational disruptions. FSPs shall develop policies, strategies, and procedures to guarantee that critical business services and operations are resumed immediately after a disruption.

1.5 The Guidelines implementation (see Figure 1) is expected to provide a structured approach to manage risk within the FSPs environment to respond and recover from risks that cannot be controlled or mitigated which can lead to damages and losses under adverse or abnormal conditions and ensure delivery of services in the event of a disruption.

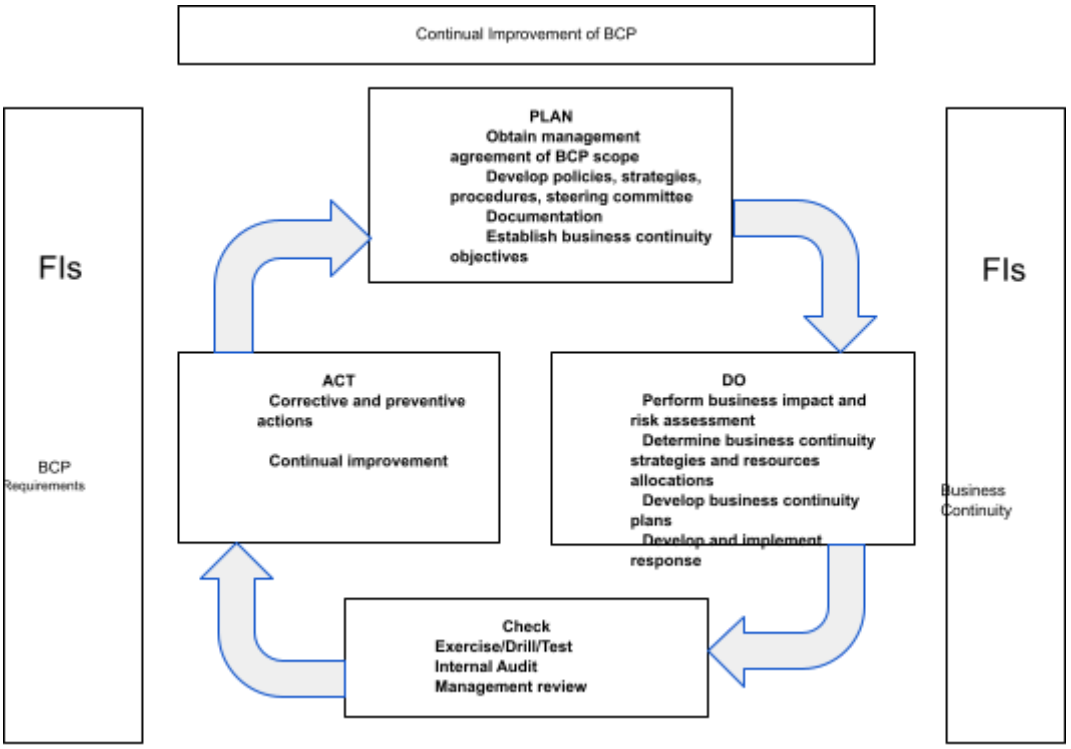

Figure 1 BCP implementation cycle

Terms and Definitions

1. **Business continuity management:** A set of procedures that includes establishing rules & regulations, guidelines, procedures, and other controls to ensure that the FSPs continue to operate in the event of operational disruptions.

2. **Business Continuity Plan (BCP):** A strategy that outlines the (1) roles and responsibilities, (2) resources, and (3) procedures required to recover from an operational disruption, fulfill the FSP's business obligations, and then return its operations to normality.

3. **Business Impact Analysis (BIA):** Analyzing operations and the impact that a business disruption may have on them.

4. **Business Function:** An action or series of activities carried out by individual organizational lines (i.e., department or unit) in the FSPs.

5. **Critical business service:** A business service that, if interrupted, has the potential to have a substantial impact on the FSP's safety and soundness, its customers, or other FSPs that are interdependent on each other's services.

6. **Dependency Mapping:** A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

7. **Maximum Tolerable Period of Disruption (MTPD):** Time it would take for adverse impacts, which might arise as a result of not providing critical business functions or performing an activity, to become unacceptable.

8. **Minimum Business Continuity Objective (MBCO):** Minimum standard of services and/or goods that the FSP will tolerate in order to accomplish its business objectives in the event of a disruption.

9. **Recovery Point Objective (RPO):** Maximum quantity of data that may be lost after recovering from a disaster, failure, or equivalent event and the lost data should be acceptable.

10. **Recovery strategies:** A planned course of action by the FSP that has been reviewed by management and tested to ensure the recovery and continuity of business services and functions in the event of operational disruptions. (e.g., internal or external hot sites, cold sites, reciprocal service agreements for alternate work areas, mobile recovery, etc.)

11. **Recovery Time Objective (RTO):** 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 minimum service level that is sufficient to meet the FSP's business obligations.

12. **Risk appetite:** Amount of risk that FSP is willing to take in pursuit of objectives it deems have value.

13. **Critical Information Infrastructure (CII):** A computer resource whose loss would severely compromise security, loss of money, or safety.

14. **Top management:** Person or group of people who directs and controls an organization at the highest level. Top management has the power to delegate authority and provide resources within the organization.

2. Critical Business Services and Functions

2.1. Business functions reinforce the provision of business services to FSP's customers. When a business function is disrupted, all of the business services that rely on it may also be impeded, thereby amplifying the operational or business impact on the FSPs. Some business functions may not directly contribute to business services, but their disruption could have an impact on a FSP's safety and soundness.

2.2. In developing recovery strategies, the FSP shall consider taking an end-to-end view of the critical business services' dependencies, considering not only the recovery of individual processes but the entire set of processes supporting the service's delivery. This will minimize disruption, protect customer interests, and keep the FSP safe and sound.

2.3. The FSP shall ensure a clear accountability and responsibility for the business continuity of its critical business services. In the event of a disruption, the FSPs shall designate personnel to oversee the recovery and resumption of each critical business service.

3. Risk assessment (RA) and Business Impact Analysis (BIA)

3.1. Due to time and resource limitations, it might not be feasible or viable to immediately restore all business services and functions in the case of an interruption. Accordingly, the FSPs shall decide on the most effective recovery plans and resource distribution, and prioritize the recovery of its business services and functions depending on their criticality (refer to Appendix I: Critical Information Infrastructure for RA and BIA)

3.2. The FSPs shall identify its critical business services through the Business Impact Analysis (BIA) and identify critical business services and functions (refer to Appendix III: Example for the CII mapping for Financial Sectors) by considering the impact of their unavailability on:

(a) the FSP's safety and soundness which 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);

(b) the FSP's customers, based on the number and profile of customers affected such as retail/corporate/interbank customers, as well as how they are impacted; and

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

3.3. Although there are economic benefits to centralizing operations, the operational risk may arise when there is a concentration of people, technology, or other required resources in the same zone. If numerous crucial business services and/or operations are outsourced to a single service provider, FSPs may also experience risk in terms of people, process and technology which can impact the delivery of critical business services. The FSPs are required to adopt sound and responsive risk management and recovery strategies by conducting RA and BIA on the People, Process, Technology and the environment.

3.4. The FSP shall consider adopting the following approaches to mitigate the risk in order to reduce the impact in the event of a disruption:

(a) setting up primary and secondary operation sites – to mitigate the widespread impact caused during the disruption of the critical business services and functions, the FSP need to establish a separate primary and secondary sites of critical business services and functions, or infrastructure (such as data centers and disaster recovery);

(b) segregation of critical business services and functions – to address the risk of losing several critical business services and functions concurrently in the event of a disruption;

(c) arrangements of the back-up team – to eliminate the key-person dependency, the FI should deploy critical personnel across different zones, or establish reserve team arrangements ;

(d) identification of alternative service provider – to provide immediate support when the primary service provider is unavailable; and

(f) conduction of cross-training programs – to build versatility by identifying the critical skills or roles and responsibilities required for the operation of the critical business services and functions.

4. Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO)

4.1. Based on the BIA results, the FSPs shall determine the Minimum Business Continuity Objective (MBCO), Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO) for each critical business function. The goal is to develop a BCP that details the procedures and the minimum level of resources required to recover the critical business functions within the recovery time frame (refer to Appendix II: Maximum Tolerable Period of Disruption) and maintain services at an acceptable level.

4.2. Each critical business service should have a Recovery Time Objective (RTO) established by the FSP. As it is a time-based metric, the RTO clarifies the expected recovery timelines for each business service within the FSP. This will aid in resource

prioritization during planning, as well as decision-making and monitoring recovery progress during a disruption.

4.3. While establishing RTOs, the FI should consider its obligations to customers as well as other FIs that rely on the business services. The FSP is expected to implement recovery strategies that will allow it to meet the established RTOs and recover to the service levels required to meet its business obligations. The FSP shall ensure that the Recovery Time Objectives (RTOs) of the underlying business functions and their dependencies meet the RTOs for critical business services that are supported by multiple business functions.

4.4. When a critical business service experiences a partial disruption, the FSP shall establish clearly defined criteria for BCP activation (including intermittent or reduced performance that is not tantamount to complete unavailability of service). This will help the FSP activate its BCP in a timely and decisive manner, before the service degradation worsens to the point that results in severe impact.

4.5. The service uptime of 99.93% should be maintained for all the critical systems/ services and the allowed downtime is one hour thirty-two minutes two seconds (1h 32m 2s) quarterly. However the current acceptable downtime will be reviewed at an appropriate time.

5. Backup and recovery site

5.1. FSP shall make available a functional backup and recovery site in the event the business premises, key infrastructure and systems supporting critical business functions become unavailable.

5.2. The backup and recovery sites shall either be in-house arrangements, or available through an agreement with the recovery facility provider, or a combination of both options.

5.3. The FSP shall assess the suitability and capacity of the backup and/or recovery site to ensure that the site is:

a) sufficiently distanced from the primary site to avoid being affected by the same disaster or source of disruption;

b) using a separate or alternative telecommunication network and power grid from the primary site to avoid a single point of failure;

c) readily accessible and available for occupancy, taking into consideration the logistic requirements within the recovery time frame stipulated in the BCP; and

d) for technology requirements, the FSP shall ensure that the systems at the recovery sites are:

i) compatible with the FI's primary systems (in terms of capacity and capability as agreed to RTO, RPO, MTPD and MBCO) to adequately support the critical business services and functions; and
ii) continuously updated with a current version of systems and application software to reflect any changes to the FI's system configurations (e.g., hardware or software upgrades or modifications).

5.4. FSP shall provide a recovery facility (hot site, online mirroring, etc.), which commensurate with its established RTO/RPO/MTPD/MBCO and for critical business functions.

6. Dependency Mapping

People, Processes and Technology

6.1. With an increasing dependency on common IT systems and third parties, the financial sector has become increasingly interconnected. To mitigate the risk associated with these linkages, the FSP shall identify and map the end-to-end dependencies that support each critical business service, including people, processes, technology, and other resources (including those involving third parties).

6.2. The dependency mapping will permit the FSP to identify resources that are critical to service delivery, consider the implications of their unavailability, and address any gaps that may impede the effective and safe recovery of critical business services. The information derived from the dependency map should be used by the FSP to ensure that the recovery of the business function and its dependencies meet the established RTOs.

Third-Party Dependencies

6.3. Some FSPs engage third parties to support the delivery of their critical business services. These arrangements could increase operational risks due to a third party's failure, delay, or compromise in providing the service.

6.4. FSP shall put in place measures that enable third parties to meet the RTOs of its critical business services. This can be done through measures, such as the following:
(a) Identify and review critical outsourcing partners and ensure that the accountability and liabilities are clearly drawn in the Service Level Agreements (SLA) during service disruptions or crises.
(b) establish and regularly review operational level or Service Level Agreements with third parties that set out specific and measurable recovery expectations and support the FSP's BCP;

(c) review the BCPs of third parties and verify that the BCPs meet appropriate standards and are regularly tested;
(d) establish arrangements with third parties to safeguard the availability of resources, such as requesting for dedicated manpower;
(e) conduct audits on the third parties; or
(f) perform joint tests with third parties.

6.5. FSP shall also put in place plans and procedures to address any unforeseen disruption, failure, or termination of third-party arrangements to minimize the impact of such adverse events on the continuity of its critical business services.

6.6. As far as possible, the FSP shall put in place measures to address the disruption of common utility services supporting critical business services, such as implementing redundancy or alternative contingency arrangements.

7. Continuous Review and Assessment

7.1. BCP is an ongoing effort to ensure that the measures put in place can address operational risks posed by current threats as well as potential future threats. FSPs shall take a proactive approach to business continuity by incorporating BCP into its day-to-day operations to address a wide range of severe and plausible disruption scenarios that may arise over time.

7.2. While globalization and technological advancement allows FSP to improve their business processes, their dependence on technology and third parties also increases their risk exposure. The FI should address and assess such risks proactively, identify areas for improvement and ensure that their BCP remains relevant and dynamic. This will enhance the FI ability to manage any unexpected disruptions to its business services. The FI should come up with the Risk Management Process (Risk Identification, Risk Assessment, Risk Treatment and Risk Monitor & review) that is reviewed periodically for the risk reconnaissance and proactive treatments to avoid unanticipated system failure and zero-day attack.

Threat Monitoring, Review and Reporting

7.3. FSPs shall actively monitor and identify external threats and developments which might interrupt its normal operations, and should have an escalation process in place to notify internal stakeholders and senior management about relevant threats in a reasonable timeframe.

7.4. FSPs shall include processes for conducting environmental scanning for relevant risk events such as natural disasters, terrorism, pandemic outbreaks, and cyber incidents. FSPs

shall also pay attention to public advisories issued by relevant authorities to get the latest information and guidance on emerging threats that may hinder their business operations.

Ongoing assessment

7.5. Following an operational disruption, FSPs shall conduct a review to identify areas for improvement and to fill any gaps in its BCP measures.

7.6. FSPs shall regularly assess the need for additional tools and automation to enable it to manage an incident or disruption more effectively. These can include implementing tools that enhance the FSP's BCP implementation or crisis management, such as automated workflows, templates and checklists, communications tools for activation and notification of personnel, as well as situational dashboards providing real-time updates on the incident.

7.7. FSPs shall update its BCP policies, plans, and procedures, including relevant training programs 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 RTOs and dependencies at least annually, or whenever there are material changes that affect them.

8. Exercising and Testing of BCP

8.1. Testing of the BCP is crucial in validating an FSP's preparedness. FSPs shall identify the critical business services based on the criticality and sensitivity of the systems and functions, and accordingly, conduct comprehensive testing of the BCP **half-yearly— for the critical business services** and **yearly— for the non-critical business services** in order to gain assurance on the robustness of the BCP in terms of response and recovery to the service level in delivering critical business services and meeting the FSP's business obligations.

8.2. All components of a business process should be meaningfully tested (e.g., from frontline through to supporting and processing components, etc.). This shall include testing the connectivity, functionality and load capacity of the infrastructure provided at the recovery site(s). FSPs shall satisfy themselves that their exercise programs adequately cover both the qualitative (e.g., response time, etc.) and quantitative (e.g., volume capacity, etc.) aspects.

8.3. FSPs shall progressively make their exercises more challenging and introduce different scenarios each time they conduct the same type of exercise. This would lead to an increase in confidence in their business continuity preparedness.

8.4. The scope of BCP exercise may include but is not limited to:

(i) Desktop walk-through exercise to full system test;
(ii) Staff call-tree activation (with and without mobilization);
(iii) Back-up site to back-up site exercise (including with it or disaster recovery service providers);
(iv) Alternative arrangements of shared services;
(v) Back-up storage medium restoration;
(vi) Retrieval of vital records;
(vii) Sensitize senior management and staff involved in crisis management (concerns and practice making decisions under simulated conditions); and
(viii) Verify that the RTOs of its critical business services and RTOs of its critical business functions can be met through the established recovery strategies.

8.5. FSPs shall select the types of tests that best meet these objectives, and set out the frequency and scope of these tests to be commensurate with the criticality of the business services and functions. FSP shall 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 FSP's business continuity testing should be reported to the senior management.

Remedial actions

8.6. 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. FSP shall 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.

9. Audit

9.1. BCP audit is an important means to provide the FSP with an independent assessment of the adequacy and effectiveness of the implementation of its BCP framework. FSP shall ensure that its audit program adequately covers the assessment of BCP preparedness based on the level of operational risks that it is exposed to.

9.2. FSPs shall audit its overall BCP framework and the BCP of each of its critical business services at least once every year. The audit shall assess the adequacy and effectiveness of the FI's BCP. The audit shall pay particular attention to higher risk areas identified from the FSP's risk assessment, previous audit findings, and relevant incidents.

9.3. FSPs should obtain BCMS certification through the BCP audits conducted by a qualified party who possesses the requisite BCP knowledge and expertise to perform the audit and is independent of the unit or function responsible for the BCP of the FSPs.

9.4. FSPs should establish processes to track and monitor the implementation of sustainable remedial actions in response to the audit findings. The FSP shall escalate any significant audit findings on lapses that may have a severe impact on the FI's BCP to the Board and senior management. The FSP shall submit the BCP audit reports to RMA upon request.

10. Incident and Crisis Management (Major Incident Handling and Escalation Strategy)

Incident Management

10.1. The FSP shall have robust processes to manage incidents in order to resume critical business services and functions within the stipulated 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

10.2. The FSP's senior management is responsible for steering the FSP out of a crisis by overseeing its crisis management activities. To aid the senior management in responding to a crisis, the FSP shall 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 FSP 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

10.3. The FSPs shall have in place communication channels such as hotlines, email, instant messaging apps, etc., to update staff on developments during an incident or a crisis. This includes cascading timely information that staff shall take note to protect their safety, as well as sending out messages on staff welfare to manage staff morale.

Communications with External Stakeholders

10.4. The FSP should ensure that communications to its external stakeholders are proactive, transparent, and factual. This will reassure stakeholders and maintain customer confidence during a disruption or crisis.

10.5. To facilitate timely public communications, the FSP shall 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 FS shall also coordinate with peer FSPs through the relevant industry associations to achieve consistent messaging to the public in the event of widespread disruption. The FSP shall also identify its designated spokesperson(s) who will be responsible to address the media and the public.

10.6. The FSP shall ensure that RMA is notified via email to bcp@rma.org.bt as soon as possible, but not 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. In the notification, the FSP shall provide information as per the RMA incident reporting template (attached Annexure I), such as the assessed impact to its customers and the actions that have been taken (e.g. activation of alternative service channels, backup sites or manual procedures, public communications, etc.)

11. Roles and Responsibilities of Board and Senior Management

11.1. Board and senior management are ultimately responsible for the FSP's business continuity. A prolonged disruption in the performance of the FSP'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.

11.2. The Board approves the Business Continuity Policy of a bank. Senior Management is responsible for overseeing the BCP process which includes:

- Determining how the institution will manage and control identified risks

- Allocating knowledgeable personnel and sufficient financial resources to implement the BCP
- Prioritizing critical business functions
- Designating a BCP committee who will be responsible for the Business Continuity Management
- The top management should annually review the adequacy of the institution's business recovery, contingency plans and the test results and put up the same to the Board.
- The top management should consider evaluating the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.
- Ensuring that the BCP is independently reviewed and approved at least annually
- Ensuring employees are trained and aware of their roles in the implementation of the BCP
- Ensuring the BCP is regularly tested on an enterprise-wide basis
- Reviewing the BCP testing program and test results on a regular basis and
- Ensuring the BCP is continually updated to reflect the current operating environment

11.3. The Board and senior management should therefore provide the leadership and strategic direction to establish strong governance over the FSP's BCP. This would ensure that the FI has the ability to effectively respond to and recover from a wide range of operational disruptions.

11.4. The Board and senior management should build an organizational culture that has business continuity preparedness embedded within the FSP's day-to-day risk management, and integrated within the FSP's operational risk management framework to enable effective identification and management of the risks across the organization.

Board of Directors

11.5. The Board of Directors delegated shall be responsible to ensure that:

- an effective and comprehensive BCP framework is established and maintained to manage potential operational disruptions and to meet its business needs and obligations;
- BCP function or equivalent is established and sufficiently resourced to oversee the organization-wide implementation of the BCP framework to achieve the desired state of business continuity preparedness;

- the effectiveness of the BCP 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
- an independent audit is performed to assess the effectiveness of controls, risk management and governance of business continuity preparedness of the FSPs.

11.6. Allocating knowledgeable personnel and sufficient financial resources to implement the BCP and Designating a BCP committee who will be responsible for the Business Continuity Management to:

- Ensure that the BCP is independently reviewed and approved at least annually;
- Ensure employees are trained and aware of their roles in the implementation of the BCP
- Ensure the BCP is regularly tested on an enterprise-wide basis
- Review the BCP testing program and test results on a regular basis and
- Ensure the BCP is continually updated to reflect the current operating environment

Senior Management

11.7. Senior management, who is responsible for executing the FSP's BCP framework, has sufficient authority, competency, resources, and access to the Board.

11.8. The senior management should ensure that:

- the BCP 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;
- sound and prudent policies, standards and procedures for managing operational disruptions are established and maintained, and standards and procedures are implemented effectively;
- roles and responsibilities for maintaining the FSP's business continuity preparedness are established and defined clearly;
- measurable goals and metrics are used to assess the FSP's overall business continuity preparedness;
- business services and functions that are critical to the FSP are identified, their roles are commensurate with its business needs and obligations;
- 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 RTOs;
- gaps and weaknesses identified from the FI's business continuity testing, post-mortems of incidents, audit, or other risk management programs (e.g., risk and control self-assessments) are remediated in a timely manner; and
- A training program is established and reviewed annually to ensure that all staff who have a role in the FSP's BCP are familiar with their roles and responsibilities.
- Prioritizing critical business functions

11.9. The senior management should annually review the adequacy of the institution's business recovery, contingency plans and test results and put up the same to the Board.

11.10. The senior management should consider evaluating the adequacy of contingency planning and periodic testing by service providers whenever critical operations are outsourced.

11.11. Develop an enterprise-wide BCP and prioritization of business objectives and critical operations that are essential for recovery.

11.12. Regular update of business continuity plans based on changes in business processes, audit recommendations, and lessons learned from testing and considering all factors and deciding upon declaring a "crisis".

11.13. The senior management should provide an annual attestation to the Board on the state of the FI's BCP preparedness, the extent of its alignment with the Guidelines, and key issues requiring the Board 's attention such as significant residual risk. The attestation shall also be provided to RMA upon request.

- Appendix I: Critical Information Infrastructure for RA and BIA

#	Criteria	Description
1	Population Affected	The percentage of the population of the sector affected from the disruption of the service
2	Geographic Concentration	The geographic area that could be affected by the loss or unavailability of a critical services
3	Operational Impact	The daily operations of the public, such as making payments/fund transfers, are stopped or prevented
4	Financial Impact	The revenue loss from the disruption of the service
5	International Businesses	The effect that a service interruption will have on the international businesses, such as international payments and remittances
6	Service Usage	The daily usage of the services by customers
7	Service Uptime	The minimum uptime required to avoid critical service disruption
8	Third Party Dependency	Inter-dependencies within and outside the sector (unavailability of power and internet connectivity)
9	Public /Consumer Confidence	The effect that disruption/unavailability of this service will have towards the (banking) sector
10	Public Order	The effect that interruption or unavailability of banking systems will have on the public, systems and processes
11	Maintainability	Information asset that is most expensive to replace/protect
12	Liability	Information asset's loss/compromise that would cause the most embarrassment or cause the greatest liability.

- **Appendix II: Maximum Tolerable Period of Disruption (MTPD)**

Sl .no	Component	Uptime	Downtime (Quarterly)	MTPD
1	Infrastructure/Network/Data Center	99.93 %	1h 32m 2s	2 hrs
2	Core Banking Software	99.93 %	1h 32m 2s	2 hrs
3	Internet Banking	99.5 %	1h 32m 2s	2 hrs
4	Bhutan Financial Switch	99.93 %	1h 32m 2s	2 hrs
5	Bhutan Immediate Payment Services (BIPS)	99.93 %	1h 32m 2s	2 hrs
6	BIRT-Fund Transfer	99.93 %	1h 32m 2s	2 hrs
7	Society for Worldwide Interbank Financial Telecommunications (SWIFT)	99.93 %	1h 32m 2s	2 hrs
8	Cheque Truncation System(CTS)	95 %	4d 13h 34m 21s	3 hrs
9	Loan Services	95 %	4d 13h 34m 21s	3 hrs
10	Pension Services	90 %	9d 3h 8m 43s	4 hrs
11	Funds and Investment Services	95 %	4d 13h 34m 21s	3 hrs
12	Insurance Services	99 %	21h 54m 52s	2 hrs
13	Remittance Services	99.93 %	1h 32m 2s	2 hrs
14	Others (office management and utility services	99.93 %	1h 32m 2s	2 hrs

- **Appendix III: Example for the CII mapping for Financial Sectors**

Sector	Critical Services	Asset	Asset Description	*Population Affected*	*Geographical Concentration*	*Operational Impact*	*Financial Impact*	*International Businesses*	*Service Usage*	*Service Uptime*	*Third Party Dependency*	*Maintainability*	*Liability*	*Public / Consumer Confidence*	*Public Order*
Financial Institutions	Banking and Payment Services	Core Banking Software	Banking software to provide Loans and Deposits services to Customers	H	H	H	H	H	H	H	H	H	H	H	H
		Internet Banking	Platform to avail Banking services and money transfer facilities across the Banks and Agencies.	H	H	L	L	L	L	L	H	H	H	L	L

		Bhutan Financial Switch (BFS)	Interoperability of ATM cards and Point of Sales (POS) among the banks	H	H	H	H	H	H	H	H	H	H	H	H
			Bhutan QR Code is a unique platform to facilitate low-cost interoperability of QR Code payments	H	H	H	H	H	H	H	H	H	H	H	H
		Bhutan Immediate Payment Services (BIPS)	Interoperability of retail payment across the banks and agencies (mPay, mBoB, Tpay, Epay myRICB,mBIL, etc.).	H	H	H	H	H	H	H	H	H	H	H	H
		BIRT-Fund Transfer	High value fund transfer across the banks in Bhutan. Example:	H	H	H	H	H	H	H	H	H	H	H	H

			Disbursement of salary, welfare, etc.												
		Society for Worldwide Interbank Financial Telecommunications (SWIFT)	For international fund transfers	H	H	H	H	H	H	H	H	H	H	H	H
		Cheque Truncation System(CTS)	Clearing of interbank cheques	H	H	H	H	L	H	M	H	H	H	H	H
	Loan Services	Loan Management System	Loan application and approval	H	H	H	H	H	H	H	H	H	H	H	M
	Pension Services	Pension Management System	Manages pension and PF for civil servants and pensioners	M	M	H	M	L	L	M	H	H	H	M	M
	Funds and Investment Services	Real estate and mutual fund	Manages real estate and fund investment, shares and bonds	H	H	H	H	L	H	H	H	H	H	H	H

	Insurance Services	Insurance Application System	General Insurance Application	H	H	H	H	H	H	H	H	H	H	H	H
	Remittance Services	Remittance System(Money Gram, Western Union, Ria, RemitBhutan system, etc.)	Platform to receive remittance from anywhere in the world.	H	H	H	H	H	H	H	H	H	H	H	H
	Infrastructure/Network/Data Center	Servers, Storages, Switches, AC, Firewall, UPS, Generator, Load balancer,Routers etc.	Network, hardware, power backup systems, storages required to host application and systems for provide uninterrupted services	H	H	H	H	H	H	H	H	H	H	H	H
	Others (office management and utility	Email Server	Notifications, OTP shared through email to those customers who are residing outside	H	H	M	L	H	H	H	H	H	H	H	H

	services)		Bhutan												
		SMS Gateway	OTP transaction notification and authentication to customers	H	H	M	H	H	H	H	H	H	H	H	H
		IP telephony	Communication platform	L	L	L	L	L	L	L	L	L	L	L	L
Severity Level H: High M: Medium L: Low Example: Bhutan Immediate Payment Services (BIPS) will have High impact on the CII															

- Annexure I. Incident Reporting Template

Instructions:

	All Incidents
1. Incident Notification to RMA (as soon as possible, within an hour and email to bcp@rma.org.bt)	· Submit Section (A) of this Incident Reporting Template
2. Subsequent update(s) to RMA (updates to be provided as and when there are changes in the current situation, or as requested by RMA)	· Submit any updates to Section (A)
3. Full Incident Report to RMA	· Submit Section (A) and (B)

Section (A) Items 1 to 3	
1. Particulars:	
· Date and Time of Notification to RMA	

· Full Name of Institution	
· Name of Caller/Reporting Staff	
· Designation/Department	
· Contact details (email, mobile)	
2. Details of Incident:	
· Discovery date and time of incident	
· Nature of incidents, affected areas: (i) Outage of IT system (*e.g. core banking systems, ATMs, POS, Domestic Payments such as NQRC, BIPs, BIRT-Fund Transfer, Payment Gateway, Internet Banking, CTS, RuPay, International cards, etc.)* (ii) Warnings of cyber-heist *(e.g., Hacking or malware infection against FI's system, web defacement, distributed denial of service attacks)* (iii) Theft or Loss of Information *(e.g., sensitive/important/customer information stolen or missing from business locations)* (iv) Unavailability of Infrastructure or work premises *(e.g., Power blackout, telecommunication linkages down, fire in office buildings and the affected locations.)*	

(v) Unavailability/shortage of Staff *(e.g. High absenteeism leading to BCP activation)* (vi) Others (e.g. *Unavailability of service providers, breach of laws and regulations)*	
· What actions or responses have been taken by the institution (short term, Mid Term & Long-term measures)	
3. Impact Assessment (examples are given but not exhaustive):	
· Business impact including availability of services – Treasury Services, Cash Management, Trade Finance, Branches, Core Banking System, ATMs, POS, Payment Gateway, Internet Banking, BIRT-Fund Transfer, Clearing and Settlement activities etc.	
· Stakeholders' impact – affected retail/corporate customers, affected participants including operator, settlement institution and service providers etc.	
· Financial and market impact – transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds etc.	
· Reputational impact – is the incident likely to attract media attention?	
· Regulatory and Legal impact	
Section (B) Items 4 to 6	

4. Detailed chronological order of events:	
· Date of incident, start time and duration.	
· Escalation steps taken, including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
· Stakeholders informed or involved	
· Various channels of communications involved	
· Rationale on the decision/activation of BCP and/or IT DR	
5. Detailed Root Cause Analysis:	
· Factors that caused the problem/ Reasons for occurring	
· Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and	
· Steps identified or to be taken to address the problem in the longer term.	
6. Final assessment and remediation:	

· Conclusion on cause and effects of incident	
· List the corrective actions taken to prevent future occurrences of similar types of incidents	
· Target date of resolution_____ (DD/MM/YY).	