Business Continuity Management Disclosures

ESAF Small Finance Bank Limited ("the Bank") is a public limited company incorporated in India on 05th May, 2016 under the provisions of Companies Act, 2013. The Bank received in principle approval from Reserve Bank of India ("RBI") to establish a Small Finance Bank in the private sector under section 22 of the Banking Regulation Act, 1949 on September 16, 2015, received the license from the Reserve Bank of India on November 18, 2016 and commenced its banking operations from March 10, 2017. As per RBI Approval, the name of the Bank is included in the Second Schedule to the Reserve Bank of India Act, 1934 with effect from 12 November 2018.

The Bank is headquartered at Thrissur, Kerala, and provides services in urban, semi-urban and rural areas of the country, through its inclusive banking initiatives. The Bank provides micro, retail and corporate banking, para-banking activities such as debit card, third party financial product distribution, in addition to Treasury and permitted Foreign Exchange Businesses. The Bank does not have any foreign operations.

1. Introduction

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organization, and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. The Business Continuity Management systems consists of interrelated elements that are used to establish, implement, operate, monitor, review, maintain, and improve the business continuity processes. The system shall comprise the organisational structure, policies, plans, responsibilities, procedures, processes, and resources for business continuity management

Business continuity planning is the process through which the Bank establishes the capabilities necessary to protect its assets and continue key business processes during and after a disaster, an unexpected business interruption, caused by natural or man-made events.

2. ESAF SFB Business Continuity Plan & Framework

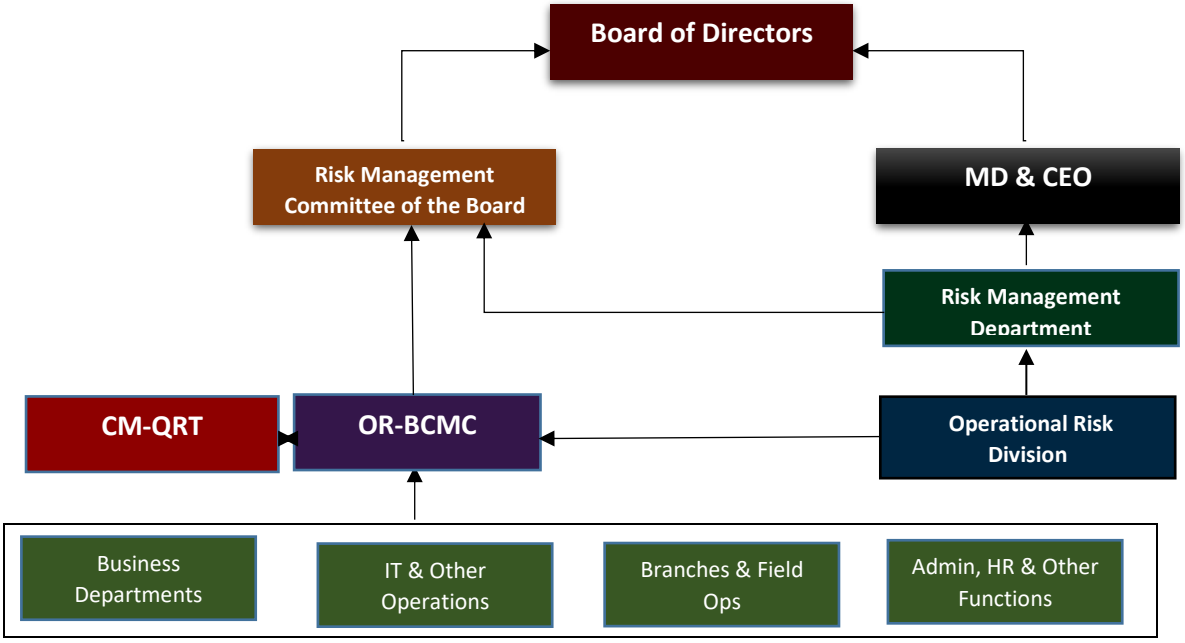
The Bank has established Business Continuity Management (BCM) plans and procedures to maintain critical operations, in the event of any kind of disruptions. BCM plans ensure that customers' requirements are met to the maximum possible extent, in case of occurrence of disruptive events. It is also intended to safeguard the security and integrity of transaction/account data and customer information. The Business Continuity Plans of the Bank has been drawn up, taking into consideration all known types of disruptive events, while concurrently accounting for the probability of unknown events. It incorporates the entire spectrum of activities that would help to ensure maintenance of effective frameworks for creating resilience, and for framing responses that safeguards and maintains critical operations, the interests of its key stakeholders, reputation, brand and value creating activities, in case of occurrence of disruptive events. The BCM framework is designed to be dynamic, to cope with the fluid and evolving nature of disruptive events. It has also been ensured that the plans and procedures comply with the guidelines and stipulations that Reserve Bank of India has laid out. The Business Continuity Plan is structured to ensure that the main focus of efforts is on clear communication of the issues to the Bank's customers in general, and specifically to the affected segments, and to ensure that alternate

arrangements are made to continue the required levels of service till the regular operations are restored.

The Bank has an effective and forward-looking business continuity framework to deal with the impact of potential disruptions. The Bank has a Board approved Business Continuity Management Policy. At the apex level the Business Continuity measures are governed by the Board of Directors and assisted by the Board Level Risk Management Committee of the Board (RMCB). The Operational Risk & Business Continuity Management Committee (OR-BCMC) is the Executive Level committee dealing with Business Continuity. The Committee also functions as the apex committee for Crisis Management and Disaster Recovery in the Bank. The Crises Management and Quick Response Team (CM –QRT) functions under the OR-BCMC; takes responsibility and acts swiftly in case of any breakdown/ failure of critical systems, occurrence of natural disasters/ accidents or any other events affecting business continuity. The OR-BCMC is convened by the Operational Risk Division functioning under the Risk Management Department of the Bank.

The different Departments and functions of the Bank have their own Business Continuity Plans. The critical functions of the Bank including IT, Operations and Treasury and their interconnections and interdependencies, including those regarding third parties and vendors conduct BCP exercises and drills at periodic intervals and the reports are placed before the OR-BCMC. The Disaster Recovery Site (DRS) of the Bank is tested with planned and unplanned drills at periodic intervals. Crisis Management and Quick Response Teams are also formed at Cluster and Branch levels. At the Cluster/Branch level, the Bank's Business Continuity Plans are intended to ensure that the basic and most critical customer service functions are maintained at the minimum acceptable levels in the event of disruptive occurrences. The Business Continuity Plans also guide mapping of branches to proximate alternate locations that would provide the basic services to customers of a branch affected by disruptive incidents. The Bank's operational resilience efforts are appropriately harmonised with the bank's business continuity plans for the delivery of critical operations and critical third-party services.

Business Continuity Framework



3. Third-party Dependency & Business Continuity Management

The third parties engaged by the Bank are vendors for outsourcing certain goods and services and Business Correspondents (BC) for various business activities. Prior to entering into such arrangements, the Bank verifies whether the third party/ Vendor/ BC have the operational resilience to safeguard the bank's critical operations. The Bank also formalises through written contractual agreements detailing how to maintain operational resilience in the event of disruptions. The Bank has in place appropriate policies and strategies for business continuity and exit strategies to maintain operational continuity in the event of a failure or disruption at a third party impacting the provision of critical operations. As part of the Bank's business continuity policy, all third parties are reviewed and assessed at least on an annual basis for their performance and systems, based on which, decisions are taken regarding continuation or termination of relationship. The Bank's Disaster recovery and Business continuity plans address the critical services for which Vendors/ BCs have been engaged

As a matter of policy, the Bank insists that the Vendors/ BCs develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures and assesses the ability of Vendors/ BCs to implement their disaster recovery and business continuity plans and ascertains whether their plans align with those of the Bank. . In case of IT related outsourcing, Business Continuity Plans includes areas like response to Cyber-attacks, network disruption and security, software or application failures, sabotage, backups and Disaster Recovery measures including DRs, Conducting DR drills etc. Vendors periodically test the Business Continuity and Recovery Plans. The Bank runs regular mock drills/joint testing and recovery exercises with the Vendors to assess Business Continuity preparedness, wherever considered necessary. In order to mitigate the risk of unexpected termination of any outsourcing agreement or insolvency of the Vendor, the Bank retains an appropriate level of control over the outsourcing with the right to intervene with appropriate preventive/corrective/deductive measures to continue the business operations in such cases, without any break in the operations or services to the customers.

4. Business Continuity Plan – Key Components

The Key components of the Bank's Business Continuity Plan are:

i. Conditions for activating plans: - which describes the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated.

ii. Emergency procedures: - which describes the actions to be taken following an incident which jeopardises business operations and/ or human life. This includes arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire service, health-care services and local government.

iii. Fall back procedures: - which describes the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales.

iv. Identification of information: - which specifies the information to be backed up and the location for storage, as well as the requirement for the information to be saved for backup purpose on a stated schedule and compliance therewith.

v. Resumption procedures: - which describe the actions to be taken to return to normal business operations.

vi. Maintenance schedule: - which specifies how and when the plan will be tested and the process for maintaining the plan.

vii. Awareness and education activities: Designed to create understanding of critical banking operations and functions, business continuity processes and ensure that the processes continue to be effective.

viii. The responsibilities of individuals: - describing who is responsible for executing which component of the plan. Alternatives are nominated as required.

5. Technology aspects of Business Continuity Plan

There are many applications and services in banking system that are highly critical in nature. High availability and fault tolerance of these are considered while designing and implementing the BCP. This aspect has been taken into account especially while designing the data centre solution and the corporate network solution.

5.1 Data Recovery Strategies

The BCP policy of the Bank provides key metrics of Recovery Point Objective and Recovery Time Objective for business processes:

i. Recovery Point Objective (RPO) –The acceptable latency of data that will be recovered.
ii. Recovery Time Objective (RTO)–The acceptable amount of time to restore the function.

Recovery Point Objective ensures that the Maximum Tolerable Data Loss for each activity is not exceeded. The Recovery Time Objective ensures that the Maximum Tolerable Period of Disruption (MTPD), for each activity is not exceeded. The metrics specified for the business processes are mapped to the underlying IT systems and infrastructure and also incorporated in contractual agreements with the Vendors providing the IT services. The Disaster Recovery Plans are then based on these metrics.

5.2 Redundancies & fall-back Options for the Technological Environment

In order to maintain business continuity, even in the event of breakdown or failure of any of the critical systems, adequate redundancies are built in to the technological environment. The redundancies built therein cover the critical applications as identified in the Business Impact Analysis. The redundancies and the fall-back options are detailed and documented in the Information Technology Services Continuity Plan (ITSCP) of the Bank covering the following aspects:

i Network Infrastructure
ii Data Centre & Disaster Recovery Sites
iii IT Infrastructure for Critical Applications
iv IT Security Infrastructure

5.3 Archival and Backup of Information/ Data

Information/ data may be lost due to failures or neglect in storage, transmission, or processing. Loss of data/ information may be caused by intentional or unintentional actions, failures, disasters, crime etc. Backup refers to the copying and archiving of data so as to restore the originals after a data loss event. To lower the risk due to loss of information/ data, both in physical and electronic forms, archival and backup of records are essential. Hence, backup and archival procedures are an integral component of the Business Continuity Plan of the Bank. The Information Systems Policies lay down the standards for maintenance of data and backups related to IT systems.

5.4 BCP for Information and Cyber Security threats

The Bank has implemented a 24 X 7 Security Operations Centre (SOC) to perform the task of detection and analysis of all potential incidents and notify the application owners which are affected, for the containment, eradication and recovery from the incident. All cyber

security incidents are recorded and reported to the departments in charge of Information Security. The Information Systems of the Bank are subjected to Vulnerability Assessment and Penetration Testing (VAPT) on a periodical basis, as a preventive measure against cyber-attacks that could threaten the confidentiality, integrity and availability of data and the systems. This ensures continuity of Business under Cyber threat situations.

6. Business Continuity and the Covid19 Pandemic

The Bank has been proactive in dealing with the biggest operational threat, i.e. the Covid19 scenario. The Bank Initiated Business Continuity measures from 6th March 2020 and convened regular meetings of the Crisis Management and Quick Response Team (CM-QRT). Various circulars, advisories and Business Continuity Plan documents are prepared on the Covid19 scenario both during the first wave and the second wave and guidelines and Business continuity measures have been circulated to the business functionaries, branches, offices and employees. Communications and advisories are issued on a regular basis to the business units, control and support functions, business correspondents and members of staff. The Bank has remained in continuous contact with customers and staff though helpdesk and customer calls to address disruptions to customer service and related functions, while taking care of the members of staff and their health. The Disaster Recovery systems are being tested periodically and monitored continuously. Network connectivity and hardware availability across the Bank are ensured. Smooth functioning of ATMs is ensured by centralised monitoring and uninterrupted cash replenishment.

The Key components of the Bank's Business Continuity Planning on account of Pandemic Risk are -

i. Proactive actions to reduce the likelihood that the Banks' operations will be significantly affected by a pandemic event, including monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, in addition to providing appropriate hygiene training and tools to employees.

ii. A comprehensive framework of facilities, systems and procedures that provide the Bank the capability to continue its critical operations in the event that a large number of the Bank's staff is unavailable for prolonged periods.

iii. Initiate sharing of important instructions/ strategies with the staff members at all levels, for soliciting better response and participation and sensitizing the staff members about preventive measures/steps to be taken to contain the impact, based on the instructions and directives from the health authorities/Government, from time-to-time.

iv. Examine the impact of customer reactions and the potential demand for, and increased reliance on, online banking, telephone banking, ATMs, and call support services. Take necessary steps to encourage customers to use digital banking facilities as far as possible.

v. A testing programme to ensure that the Bank's pandemic planning practices and capabilities are effective and will allow critical operations to continue.

vi. A programme to ensure on-going review and updates to the pandemic plan so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the Bank's monitoring programme.

The Bank has been able to address the challenges of Covid19, by providing services to customers even during the most difficult times of Covid19 crisis and contained the operational disruptions, cyber security threats and associated risks. Adherence to the Covid19 protocol and documented BCP procedures has helped the Bank in successfully

managing business continuity during the Covid19 crisis. The Bank continues to monitor and manage business continuity in a structured manner by collective efforts of its workforce and top management, under the guidance of the apex level Operational Risk and Business Continuity Management Committee and the Crisis Management and Quick Response Teams.

7. Customer Communications

In situations of any major disruptions, the customers of ESAF SFB can use the Pan-India toll free number 1800-103-3723, and for NRI customers 080-4644-3723 (Paid line), if the branch in which they maintain accounts cannot be contacted for any reason. The customer service email id - customercare@esafbank.com may be also used for contacting the Bank. The Bank's customer service link in the website is available as alternate means of communication - https://www.esafbank.com/customer-service/

(Updated by Risk Management Department in May 2021)