BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

BCM and DR Policy & Procedure

Reference No.: BESSEGGEN/I&CSF/BCM&DR

Version: 1.2

30th May 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/BCM&DR		
Document Name	**BESSEGGEN BCM and DR Policy & Procedure**		
Version No.	1.1		
Document Status	Definitive		
Issue Date	08th Aug 2022		
Compliance Status	Mandatory		
Review Period	One year from the date of release or earlier if required		
Security Classification	Internal Use Only		
Distribution	Part of BESSEGGEN I&CSF		
	Name	**Role**	**Signature**
Authored by	BESSEGGEN INFOTECH LLP		
Reviewed by	Vibhu Garg	CISO	
Approved by	Vibhu Garg	CISO	
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	08th Aug 2022	Issued
1.1	14th May 2024	Reviewed
1.2	30th May 2025	Reviewed

Table of Contents

1. Overview

The BCP (Business Continuity Planning) and DR (Disaster Recovery) Policy and Procedure outlines the processes and procedures that BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") will follow to ensure that essential business operations can continue in the event of a disruption or disaster. The policy defines and establishes priorities, and outlines the steps to be taken to minimize the impact of a disaster or disruption.

2. Objectives

Identifying critical business functions, processes, and information systems, and assessing the risks and potential impact of disruptions.

- Defining strategies and plans for responding to disruptive incidents, including emergency response, business continuity, and disaster recovery plans.
- Ensuring the availability of adequate resources, infrastructure, and technology to support the execution of the BCP and DR plans.
- Regularly testing, reviewing, and updating the BCP and DR plans to ensure their effectiveness and relevance.

3. Scope

This document covers all processes related to Business Continuity Management of the BESSEGGEN for systems/process as mandated by Regulatory agencies CERT-IN, SEBI and ISO 27001:2013

4. Policy Statement:

BESSEGGEN Shall prepare and implement requirements and procedures to provide direction so that the BESSEGGEN network remains secure during any business crisis or disaster.

Refer: APPENDIX-A Information Security Business Continuity Controls ISO 27001:2013

5. Terms used and Definition:

SN	Terms	Definitions
1	**Business Continuity Plan (BCP)**	Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption
2	**Licensing**	To keep track of asset licensing, ensuring compliance with all relevant agreements, laws and regulations.
3	**Critical Business Functions**	Key business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the organization's assets, meet organizational needs, and satisfy regulations

4	**Risk**	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence Asset
5	**Criticality**	Criticality is the quality, state, or degree of being of the highest importance
6	**Risk Analysis**	A systematic use of information to identify sources and to estimate risked.
7	**Risk Assessment**	The overall process of risk analysis and risk evaluation, where risk analysis is defined as the systematic approach to identify an organization's exposure to uncertainty and to estimate the risk.
8	**Threat**	A potential to cause an unwanted incident which may result in harm to a system such as unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin
9	**Non-Disclosure Agreements (NDA)**	A legally binding document which protects the confidentiality of ideas, Designs, plans, concepts, or other commercial material.
10	**Risk Treatment**	A process of selecting and implementing measures to change, modify or lower risk
11	**Remote Access**	Ability to get access to a computer or a network from a remote Distance.
12	**Network**	A configuration of communication equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to Each other.
13	**Information Security**	A process of safe-guarding information assets from unauthorized access, modification, use, disruption, and destruction to ensure confidentiality, integrity, availability, and non-repudiation of information.
14	**Information Security Event**	An event that is caused due to any action on an Information Asset. For example, deleting a key file from a critical business system.
15	**Information Security Incident**	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
16	**Intrusion**	An uninvited and unwelcome entry into a system by an unauthorized source.

6. Roles and Responsibilities:

Key roles and responsibilities in developing Risk assessment and business function BIA and BCP-DR plans, Main team is Business Continuity Management Team (BCM) primarily responsible for all BCP and DR plans.

BCM Team

Plays a key role in initiating and developing the process of initiating RA, BIA, BCP and DR plans implementation, testing, implementing, monitoring and considering the effectiveness and further improvement actions.

- To manage communication in case of disruptions
- To conduct BCP testing once a year

- To identify and declare disaster-scenario according to the gravity of the disaster
- To enforce BCP among teams as per disaster scenarios.
- To review BCP activities including CAPA once a year
- To coordinate with outsourcing partner wherever applicable
- To facilitate resourcing

Business Owner

Primary responsibility for the BIA, including development and ongoing maintenance. This includes Writing the BIA report and holding working sessions to collect information and to achieve Consensus on the details, including impacts from potential threats and hazards.

- To execute BCP activities as per respective procedures, disaster scenario & Individual Role assignment as mentioned in BCP plan
- To coordinate with outsourcing partner wherever applicable
- To prepare BCP documentation for his/her area of responsibilities
- To support BCP testing and prepare testing outcome document

System Owner and SME (Subject Matter Expert)

Will provide support to the development and ongoing maintenance, will provide a wider Perspective, especially for impacts to operations related or interdependent functions. SME's also Help formulate more efficient and effective mitigation strategies.

CISO / Management

Review the BIA findings, verify and approve the risk-based analysis, mitigation strategies and Business Continuity Plans. Ensure training to the selected employees to handle the BCP/DR plans Effectively and timely

- To Coordinate the development and maintenance of the Organizational BCP Policy
- To facilitate functional training of the members for BCP execution
- Auditing of BCP activities as per organization policy

Emergency Evacuation Team

The Security Coordinators of each function and the Administration function head form the Emergency Evacuation Team. Responsibilities include:

- Safe and speedy evacuation of personnel
- Ensure no personnel is left in the building
- Take a headcount of their respective teams and notify

7. Information Security Aspects of Business Continuity Management:

7.1 Information Security Continuity

Objective: Information security continuity shall be embedded in the organization's business continuity management systems

7.1.1 Planning Information Security Continuity

- **Identify the critical business/service activities**
  An organization's main business activity is determined by the activity that has a critical and major impact on the revenue of the organization. The most critical activities should be shortlisted, and priorities should be set in order of restoration and redundancies.

- **Identify critical resources**
  The vital resources should be shortlisted and prioritized in order of restoration by the BCP Leader.

- **Identify people responsible**
  This would include BCP Leader, CISO and the BCP team members. Proper escalation procedure should be followed by the people involved.

- **Impart Training for Disaster Recovery**
  Proper training should be imparted to all the employees to ensure adherence to the Recovery Plans.

- **Risk Assessment:**

  BESSEGGEN shall carry out RA for all critical business processes, support resources and sites at pre- defined frequencies to identify single points of failure

  - All critical applications (applications which contain customer PII data and/ /or has financial repercussions and/or has regulatory impact) shall be assessed at least annually.
  - Based on the findings of the risk assessment, BESSEGGEN shall prioritize and implement additional controls to reduce the exposure to threats to an acceptable level.

- **BIA (Business Impact Analysis)**

  As an essential part of Continuity Risk Management Activities, the Business Owners must conduct a business impact analysis (BIA) of critical network and service operations of BESSEGGEN business and prioritize based on impact and criticality to ensure smooth operation of services

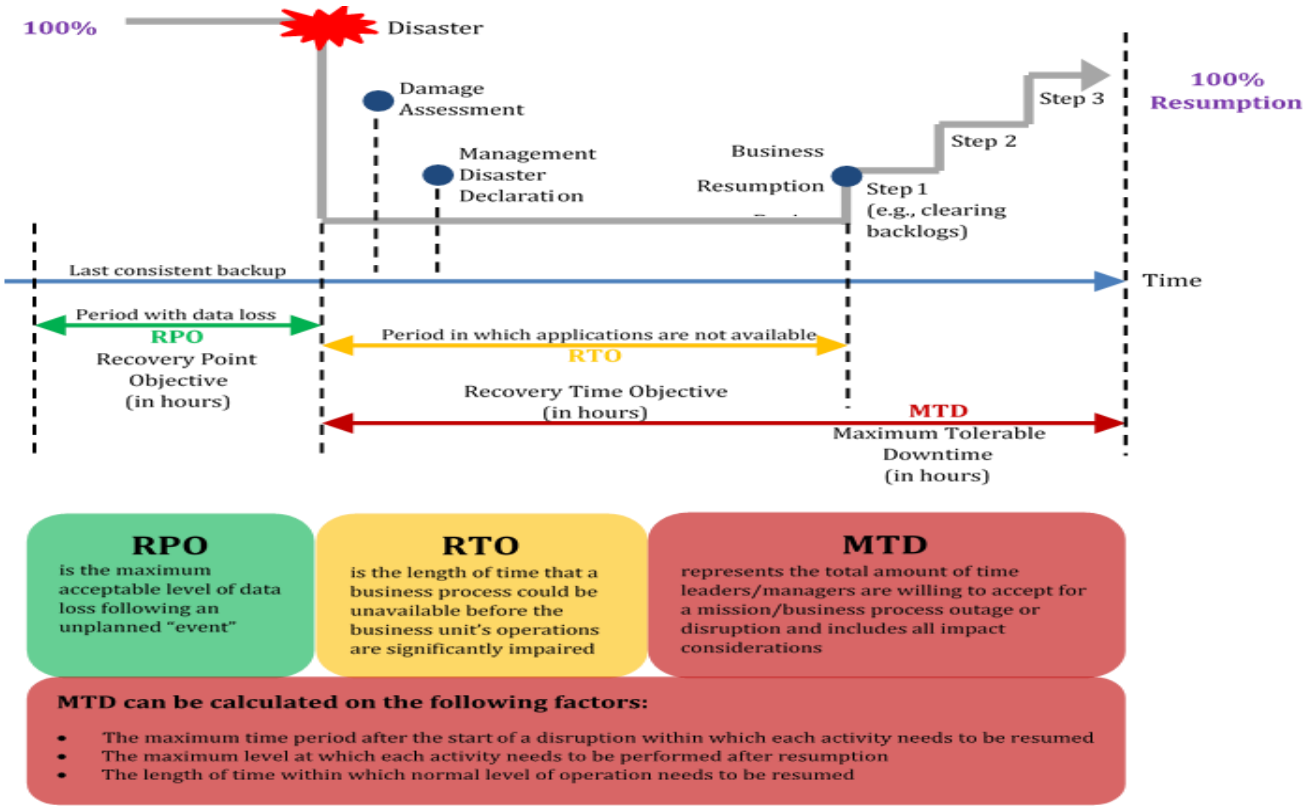
  - Validate alignment with BESSEGGEN critical Functions and essential operational activities
  - Determine the criticality of business operations/ processes through an all-hazards risk

analysis

- Identify risk mitigation and recovery strategies based on criticality

Identify resource requirements needed to resume mission/business processes and related interdependencies (facilities, personnel, equipment, software, data files, system components etc. Identify recovery priorities for sequencing recovery and resources

The BIA should help inform the Contingency Planning process in identifying preventive controls for the functions and resources, and in developing the Contingency Plan.



7.1.2 Implementing Information Security Continuity

- Plans are designed based on business impact and likelihood of occurrence severities **(Annex-B)**

Key Activities in BCP-DR recovery

- Keep BCP/DR plan approved by BCM Council
- Test the plans in a controlled environment
- Vital records are available in case of a Business Continuity (BC) event
- Recovery strategies for critical business processes shall ensure recovery within target time set for their recovery and within duration after which an organization viability will be irrevocably threatened
- The BCMS plan documentation and implementation details shall be detailed out
- Communicate to other stake holders / Regulatory bodies
- Discuss with System Owners / Subject Matter Experts
- Follow the escalation matrix in case of any doubt or delay

- In case of disaster situation, up the recovery site and route the traffic
- Ensure recovery is carried out effectively and securely
- Monitor situation and reports to concerned heads/teams
- Do RCA, Lessons Learned and steps to stop recurrence
- Changes in BCP/DR Plans for further improvement

- Disaster or disruption will be divided into three phases. These phases will follow each other Sequentially in time.

Disaster Occurrence

This phase begins with the occurrence of the disaster event and continues until a decision is made to activate the recovery plans. The major activities that take place in this phase includes emergency response measures, notification of management, damage assessment activities, and declaration of the disaster.

Plan Activation

In this phase, Business Continuity Plans are put into effect. This phase continues until the critical business functions are reestablished, and computer system services are restored. The major activities in this phase include: notification and assembly of the recovery teams, implementation of interim procedures, and re-establishment of data communications.

Restoration

This phase consists of all activities necessary to make the transition back to a normal business operation.

Emergency Response

BESSEGGEN shall have a well defined emergency response framework. Emergency response process shall involve preparing for disaster by putting in place mitigation controls as part of Pre Crisis-Preparation, disaster response (e.g. emergency evacuation, quarantine, mass decontamination, etc.), as well as supporting and recovery after a disaster;

7.2 Redundancies

Objective: To ensure availability of information processing facilities.

7.2.1 Availability of Information Processing Facilities

- Redundancy refers to implementing, typically, duplicate hardware to ensure availability of network/ information processing systems. The principle is that if one or more items fail, then there are redundant items that will take over.

- Network redundancy is introduced to improve reliability and ensure availability. The

purpose of redundancy is to prevent any disruption of customer service and business continuity in case of a technical failure or disaster by maintaining a continuity of service.

- BESSEGGEN to conduct the testing of redundant network components and systems periodically to ensure that fail-over will be achieved in a reasonable time-frame.

- Redundant components must be protected (Physically or logically) at the same level or greater than the primary components.

8. Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the CISO/Management and exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
  Evidence of approval by the CISO/Management

9 List of Appendix

ANNEX-A	Information Security Business Continuity Controls
ANNEX-B	Categorization of BCP & Disaster Events based on occurrence, likely-hood, and Business impact
ANNEX-C	Notification Plan
ANNEX-D	Business Continuity Overview
ANNEX-E	Vendor List
ANNEX-F	Employee Contact List

ANNEX-A
Information Security Business Continuity Controls ISO 27001:2013

A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
		Control
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
		Control
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
		Control
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
A.17.2 Redundancies		
Objective: To ensure availability of information processing facilities.		
		Control
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

ANNEX-B

Categorization of BCP & Disaster Events based on occurrence, Likely-hood, and Business

impact

Likelihood of Occurrence	
Low	**Unlikely:** An event/condition that can be envisioned but hasn't occurred (~20% chance over the foreseeable future)
Moderate	**Possible:** An event/condition that has occurred in the past (50:50 over the foreseeable future)
High	**Likely:** An event/condition that has occurred in the past at a frequency warranting its anticipation in in the near future (>75% chance)

Impact on Business function	
Low	**Little Impact:** Any outage with little impact, damage, or disruption to the organization.
Moderate	**Important/Moderate Impact:** Any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems.
High	**Mission-critical Impact:** The damage or disruption to the system would cause the most impact on the organization, mission, and other networks and systems.

Likelyhood	**High**	**Mitigate & Develop BCP**	**Mitigate & Develop BCP**	**Mitigate & Develop BCP**
	Moderate	**Mitigate & Develop BCP**	**Mitigate & Develop BCP**	**Mitigate & Develop BCP**
	Low	**Accept**	**Mitigate & Develop BCP**	**Mitigate & Develop BCP**
		Low	**Moderate**	**High**
		Business Impact		

SN	Problematic Event or Incident	Affected Business Process(es)	Impact Classification & Effect on finances, legal liability, human life, reputation
1	Fire - Loss/ damage to office building due to fire	Business & Operations	High, Human Life
2	Earthquake - Loss/ damage to office building due to earthquake	Business & Operations	High, Human Life
4	Hacking Attack / Virus Attack	Business & Operations	Medium, Legal Liability
5	System Failure: Server Failure	Business & Operations	Medium

ANNEX-C
Notification

S.No.	Problematic Event or Incident	Who will inform	Whom to inform
1	Fire - Loss/ damage to office building due to fire	Security Person	· Fire Service · HOD-IT · CISO · BCP Team · Security Head
2	Earthquake - Loss/ damage to office building due to earthquake	Security Person	· Fire Service
			· HOD-IT
			· CISO
			· BCP Team
			· Security Head
3	Data Centre Network Unavailable for SAP, Email & other applications	IT Shift Personnel	· HOD-IT
			· Lead IT Infra
4	Hacking Attack / Virus Attack	IT Person / End User	· HOD-IT
			· CISO
			BCP Team

ANNEX-D
Business Continuity Overview

Potential Threats and Hazards	Potential Impact	Describe Business Function Impact	Information Type(s) Impacted	Likelihood	Impact	Risk Decision	Proposed Mitigations / Actions Plan
Infrastructure Failure / Damage	Flood						
IT System Crash	Virus Attack						
Power Outage	Power is lost						
Network Failures	Communications is lost						

ANNEX-E
Vendor List

Goods / Service Provided	Vendor Name	Helpdesk Contact No. & Email Id	Service Account Manager Details	Address

ANNEX-F
Employee Contact List

S.No.	Employee Name	Function	Office Phone	Mobile No	Alternate Phone	Email	Responsibility Area
1	Ankit Pruthi	Partner					
2	Vibhu Garg	Partner & CISO					
3	Karun Singla	Partner					
4	Nishant Agarwal	Developer					
5	Prince Kumar	Developer					
6	Yogesh	Compliance Officer					