Business Continuity Management System

(BCMS)

Business Continuity Plan

Documented information Name: Business Continuity Plan

Version No: 2.0

Last Updated: 25-Jul 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

This Documented information is a confidential documented information of Sesa Group

Documented information Management Information

Documented information Title: Business Continuity Plan

Abstract: This Documented information is a Documented information of the Business Continuity Plan

Documented information Publication History

(All revisions made to this documented information must be listed in chronological order, with the most recent revision at the top)

Type of Information	Documented information Data
Documented information Title	Business Continuity Plan
Documented information Code	SESAIT/ISO22301/Business Continuity Plan
Date of Release	25-Aug 2022
Documented information Revision	25-Jul 2023
Documented information Owner	IT Department
Documented information Author(s)	Pricoris LLP
Documented information Change Reviewer	Jyoti Singh
Checked By	Dileep Singh – CISO
Security Classification	Internal Use
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature	Date Approved
1	Shobha Raikar (CDIO - IOB)	Shobha.raikar@vedanta.co.in	Electronically Approved	10-Aug 2023

Documented information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.0	22-Aug 2022	New Release	1.0	25-Aug 2022
1.1	31-Aug 2022	Changed the version no. after the stage 1 audit		03-Sept 2022
2.0	25-Jul 2023	Change in the BCMS Organization Structure Chart Added Applications in Recovery Target – Microsoft Defender, MVPL Road Dispatch Application, PRTG & VEEAM FACOR- Server Backup Remove the Application Symantec - Antivirus	Change in section 12 – Change the name of the application	10-Aug 2023

Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep K Singh	dileep.singh@vedanta.co.in

Table of Contents

1. Introduction

Sesa Goa Iron Ore (hereinafter referred to as Sesa Group), as one among the top low-cost producers of iron ore in the country, has made significant investments in Information Technology (IT) supporting its business to enhance stakeholder value, maintain market leadership and ensure customer delight. Availability of IT is of paramount importance to ensure uninterrupted business operations, and hence, Sesa Group has implemented a robust and resilient IT infrastructure for its critical applications and systems.

Sesa Group aims to design, implement, test and maintain an IT-Business Continuity Management System (BCMS) covering its key locations from where IT Services are being delivered (i.e. for processes supporting information technology). The BCMS shall cover the Primary Data Center (Navi Mumbai) and the Data Center - Head Office (Panaji, Goa).

2. Scope

This Procedure document is applicable for Vedanta Limited –Sesa Goa Iron Ore Division including SRL and SMCL in Goa, Karnataka, Odisha and Liberia, Pig Iron Division, Met Coke Division, Power Division in Goa, Sesa Coke - Vazare and Gujarat, FACOR – Odisha, Nickel Business, VGCB, Visakhapatnam referred as Sesa Group in this document.

This plan applies to all information processing systems or information assets owned/operated by Sesa Group or owned/operated by a third-party service provider on behalf of Sesa Group.

This plan applies to all the employees, contracted staff, business partners, and anyone associated with Sesa Group IT Infrastructure and applications.

3. Purpose of the documented information

Business Continuity Planning is a holistic management process, that identifies potential threats to the organization and provides a framework to build resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. Threats can be of various types, such as failure or breakdown of IT systems, communication failure, power failure, fire, earthquake, civil unrest, riots, and so on, all of which can cause a business disruption.

BCP aims to improve an organization’s resilience by proactively identifying and mitigating potential disruptions that may affect organization’s ability to continue its operations and service its customers. It prepares the organization to effectively handle such disruptions.

This document contains Sesa Group’s Business Continuity Plan (BCP). It describes the strategies, processes and procedures for Sesa Group to handle a BCP event.

A “**BCP event**” is a situation resulting in unavailability of people, facilities, and technology required to ensure continuity of IT services required by the business to continue its operations and service the customers.

This document also defines the Crisis Management Organization structure and the respective roles and responsibilities, along with recovery and resumption procedures.

This document acts as a quick reference guide to Sesa Group with respect to selecting the right action plan for a specific disaster/emergency.

The main purpose of the document is to provide a framework for following a systematic action plan when Sesa Group management decides to invoke recovery strategies during a disaster/emergency in order to:

- To provide continuity and resilience with a plan which, when executed, will permit an efficient and timely resumption of the interrupted business.
- To understand task and responsibilities of individual departments in resumption, recovery, restoration and return.
- To understand the resources required for critical departments in the recovery mode.
- To understand the vital records required for critical departments to resume business.

4. Abbreviations

- BC- Business Continuity
- BCP Business Continuity plan
- BCMS- Business Continuity Management System
- ITSE- IT Steering Committee
- CMT- Crisis Management Team
- IRT- Incident Response Team
- RTO- Recovery Time Objective
- MAO- Maximum Acceptable Outage
- BIA- Business Impact Analysis

5. Applicability

IT-BCP Applicability is limited to defining recovery and resumption procedures for threats resulting in unavailability of people, facilities, and technology required to ensure continuity of IT services required by the business to continue its operations and service the customers.

IT-BCP shall not cover:

- Business Continuity Planning for Business Processes & Support Processes (Head Office/Regional Offices/Units)
- Business Continuity Planning for Manufacturing and related processes (Plant/Supply Chain)

6. Objectives

The main objective of the plan is to

- Reduce the overall risk by limiting the impact during disruption.
- Protect the reputation of Sesa Group and adequately manage relevant stakeholders in the event of a crisis.

- Provide a structured process for resumption, restoration and recovery thereby minimizing operational interruptions to IT applications and supporting infrastructure.
- Help achieve compliance.
- Be a vehicle for rapid response.

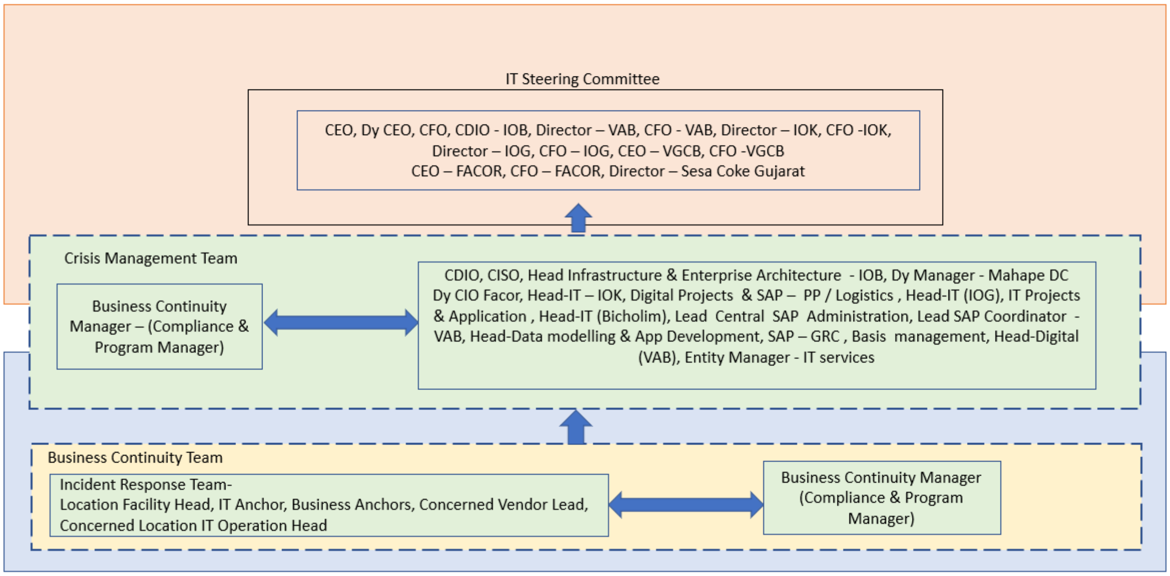
7. Assumptions

The following assumptions were considered while documenting the IT-BCP:

- The recovery strategy agreed upon is implemented and tested at periodic intervals for workability.
- Recovery of critical and significant applications is done which needs to be recovered within 24 hours.
- The incident impacting the company's primary site has not impacted the recovery arrangements. (E.g. alternate worksite, redundant supporting infrastructure, etc.)
- The identified key personnel or their backups are not physically or psychologically impacted by the incident and are in a position to carry out the recovery operations.
- Vendors/Service providers provide products/services as desired or as per the service level agreements (SLA).
- A feasible mode of transportation is available for moving personnel and goods to the recovery site.
- During any recovery period, Sesa Group will accept some degradation in support services as long as critical operations can continue.
- No two different types of incidents have occurred at the same time.
- It is assumed that a crisis will not occur simultaneously at two Data Centers at the same time, i.e., even if one datacenter is down at a time, then the other datacenter is up and running.
- The plan is based on various disaster scenarios envisaged. However, it does not include special situations that may occur. Some examples include country-wide incidents/war.

8. BCMS Organization Structure

BCMS Governance Structure


IT Steering Committee
CEO, Dy CEO, CFO, CDIO - IOB, Director – VAB, CFO - VAB, Director – IOK, CFO -IOK, Director – IOG, CFO – IOG, CEO – VGCB, CFO -VGCB CEO – FACOR, CFO – FACOR, Director – Sesa Coke Gujarat
Crisis Management Team
Business Continuity Manager – (Compliance & Program Manager)
CDIO, CISO, Head Infrastructure & Enterprise Architecture - IOB, Dy Manager - Mahape DC Dy CIO Facor, Head-IT – IOK, Digital Projects & SAP – PP / Logistics , Head-IT (IOG), IT Projects & Application , Head-IT (Bicholim), Lead Central SAP Administration, Lead SAP Coordinator - VAB, Head-Data modelling & App Development, SAP – GRC , Basis management, Head-Digital (VAB), Entity Manager - IT services
Business Continuity Team
Incident Response Team- Location Facility Head, IT Anchor, Business Anchors, Concerned Vendor Lead, Concerned Location IT Operation Head
Business Continuity Manager (Compliance & Program Manager)

8.1 IT Steering Committee (ITSC)

The IT Steering Committee is the apex of the Recovery Organization. It plays a significant role in the event of a disaster/ contingency in the form of their advice and key decisions. This team is made up of senior executives from the company who will be in charge of overseeing the recovery and resumption of mission-critical activities. The ITSC will perform a yearly review of the business continuity program of Sesa Group. Their responsibilities are as under:

8.1.1 Business as Usual

1. Establish the BCMS and ensure management commitment to process recovery in accordance with the BCP objective.
2. Set the objectives of BCMS and ensure that they are met.
3. Nominate the BCM Head with appropriate seniority and authority who will be accountable for BCM policy and implementation and facilitate the same.
4. Provide direction for efficient planning and implementation of BCMS recovery and strategies.
5. Review and approve the Business Continuity Strategy for IT Applications, Infrastructure and Services in scope.
6. Review and approve the Business Continuity Management strategy and ensure its alignment with Sesa Group’s overall strategic business continuity objectives.
7. Assign and avail the required resources to BCMS by reviewing the BCMS capabilities of Sesa Group and propose an action-plan if required.
8. To promote a business continuity culture and set the tone at the top by encouraging knowledge transfer and awareness across the company.
9. Communicating the importance of effective BCM and conformance to the BCMS requirements.

10. Obtain a clear understanding of the risks and continuity threats to business being faced by the organization and support new initiatives to improve BCMS.
11. Review and approve the recommendation of the Crisis Management Team/BCM Head.
12. Manage costs associated with Business Continuity.
13. Ensure that legal, regulatory requirements and contractual continuity obligations are identified, addressed, and achieved.
14. Review the executive summary of the audit reports.
15. Actively participate in management reviews and promote continual improvements across functions.
16. Ensure that BCM personnel's competency requirements are met and updated on a regular basis.

8.1.2 During Incident/Crisis

1. Oversight and advice to the Crisis Management Team and BC Head.
2. Review the progression of events/incidents.
3. Communication with critical customers (if required)
4. Brief Corp Comm on crisis to facilitate communication with media.

8.1.3 Authority

1. Authority to establish the policy and objectives.
2. Authority to review and approve strategy.
3. Authority to exercise oversight and advice the Crisis Management Team and BC organization during incidents.
4. Authority to approve expenses for resumption of business in case of disruption.

8.2 Business Continuity Head

1. To support the IT Steering Committee in discharging their business continuity responsibilities.
2. Develop a Business Continuity Management strategy and ensure its alignment with Sesa Group’s overall strategic business objectives.
3. Responsible for the overall direction and coordination of Sesa Group's Business Continuity Management, including Business Continuity sign-off for new investments and contracts.
4. Contributes to the corporate planning effort for specific corporate-wide Business Continuity threats (e.g.: pandemic, industrial action)
5. To facilitate Sesa Group’s response to emergencies and support the Incident Response team.
6. Ensure that lessons learnt from the incident are noted, reported, disseminated and incorporated into Sesa Group's Business Continuity Management and arrangements.

8.2.1 Authority

1. Invocation and standing down the BCP with agreement of CMT
2. Source recovery requirements to effectively manage incidents,
3. Personnel deployment.

8.3 Crisis Management Team

8.3.1 Business as Usual

1. Review and approve the risk scenarios as shared in the Crisis Management Plan.
2. Be aware of the Crisis Management Plan and Crisis Communication Plan and their role in it.
3. Participate in the exercise/test of the Crisis Management Plan.
4. Ensure that any lessons learned during the exercise/testing are shared with all stakeholders.

8.3.2 During Incidents/Crisis

1. Oversee the incident management operation and ensure the safety and security of people and assets.
2. In case the incident escalates into a crisis, provide continuous on-ground support till the crisis is averted.
3. Inform external agencies like regulators as and when the need arises. Also, liaise with service providers including security agencies, house-keeping agencies & IT service providers.
4. To analyze the situation and implement the crisis management plan to save the organization's reputation and standing in the industry.
5. Detect the early signs of a crisis before activating the crisis plan.
6. Escalate the Severity 1 incident to IT Steering Committee (ITSC), if resulting in disruption.
7. Determine and assist BC Head on invocation of BCP post consultation with relevant stakeholders based on the nature of the incident (as per the defined BCP Invocation criteria).
8. Coordinate between the various stakeholders (employees, regulators, customers, banks, shareholders, etc.)
9. In the event of a conflict, monitor the progress of activities and provide approvals as needed for resource prioritization.
10. Approve the expenses related to recovery and resumption activities.
11. Determine when to resume activities from primary location (back-to-normal).

8.3.3 Authority:

1. Authority to declare a crisis based on the criteria for declaration and invoke Crisis Management Plan.
2. Authority to communicate with regulators.
3. Authority to approve expenses related to recovery and resumption activities.

8.4 Incident Response Team (IRT)

1. Identify new risk scenarios to form part of the Crisis Management Plan.
2. Participate in exercise/test of Business Continuity Plan and Crisis Management Plan.
3. Ensure that any lessons learned during exercise/testing are reported.
4. Ensure the contact details of all stakeholders as mentioned in Contact Details are current and updated.

8.4.1 IT Anchor

IT Anchor is part of the IRT Team is responsible for the following:

1. Regular review and signoff of Maximum Acceptable Outage, Recovery Time Objective and Recovery Point Objective after coordinating with Business Anchor regarding the appropriateness of the same.
2. Identification of risks to meeting the Maximum Acceptable Outage, Recovery Time Objective and Recovery Point Objective.
3. Identify solutions and strategies for meeting the Maximum Acceptable Outage, Recovery Time Objective and Recovery Point Objective in scenarios such as people not available, premises not available, technology not available and vendor not available.
4. Identify and allocate resources (financial, technology, people, processes) required to operationalize the strategy and solutions.
5. Signoff the IT application/services' Business Continuity Plan.
6. Regular review of BIA, risks, strategy, Business Continuity Plans and contact details of key dependencies.
7. Regular review of backup plans and signoffs.

8.4.2 Business Anchors

1. To be aware of risks to continuity as shared by IT anchors.
2. To be aware of the strategy for recovery and resources required.
3. To discuss the Maximum Acceptable Outage, Recovery Time Objective and Recovery Point Objective.

8.4.3 Role of IRT During Incidents/Crisis

1. Respond to incidents causing disruption to IT services.
2. Once an incident is reported, assess the situation and, depending upon its severity, initiate an appropriate action.
3. IT Infrastructure Head to initiate communication regarding to incident at Goa to various stakeholders and Head Group Data Center to initiate communication regarding to incident at Mumbai to various stakeholders.
4. Inform external agencies like regulators, police authorities, etc., as and when the need arises. Also, liaise with service providers including security agencies, house-keeping agencies & IT service providers.
5. Instruct the IT recovery team to initiate their response procedures for IT Incidents, and the Facility & Admin Team for non-IT Incidents
6. Constantly be aware of the vulnerabilities and implement necessary security to protect the environment or assist the constituency in implementing them.
7. Contact the HR SPOC for people-related issues and to ensure the wellness of Sesa Group employees, including contract employees.
8. Ensure availability of the critical incident management infrastructure (spare IT & Networking equipment etc.) and people required for emergency operations are available.
9. Post the incident, perform a root cause analysis and identify appropriate correction & corrective actions.
10. IRT shall keep the CMT and BC Head and BC Manager duly informed about the current situation.

8.4.4 Authority:

1. To communicate with stake holders regarding incident criticality and take steps for incident response.

8.5 Business Continuity Manager

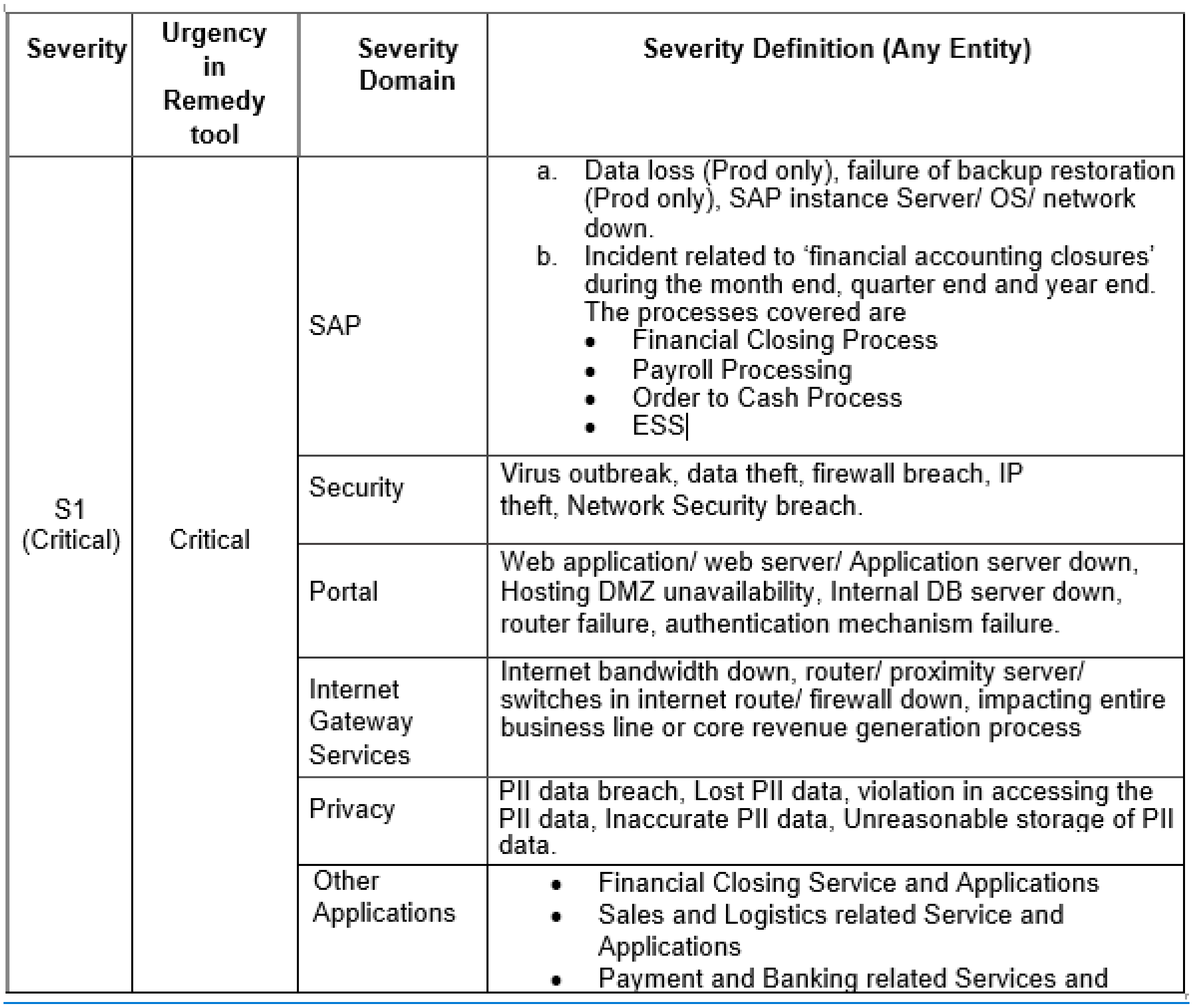
The Business Continuity Manager plays a key role in implementing the Incident Management & Business Continuity Plan and is responsible for:

1. Developing the BCMS and reviewing business continuity standards within their area of responsibility.
2. Oversee the incident management operation.
3. Escalate the Sev 1/Sev 2 incident (refer Incident Management Procedure) to the Crisis Management Team/IT Steering Committee (ITSC), where required.
4. Provides direction and support to the company in business continuity development, training, exercise and delivery.
5. Review and update BCMS documentation on a regular basis and whenever a business process changes.
6. Review the IT application plans to ensure they integrate with the overarching plan structure.
7. Develop the annual Business Continuity management plan of Sesa Group for submission to the Committee for review and approval.
8. Organize, run and/or advise on Business Continuity rehearsals, focusing on:
    - Lack of people
    - Loss/lack of facilities
    - loss of resources (technology & systems)
    - Loss/lack of supplier
9. Collate and report on the status of overarching Business Continuity threats in the Sesa Group.
10. Report the lessons learnt from the incident/crisis and update the relevant plans and arrangements.
11. Provide the performance dashboard for BCMS to the ITSC on an annual basis.

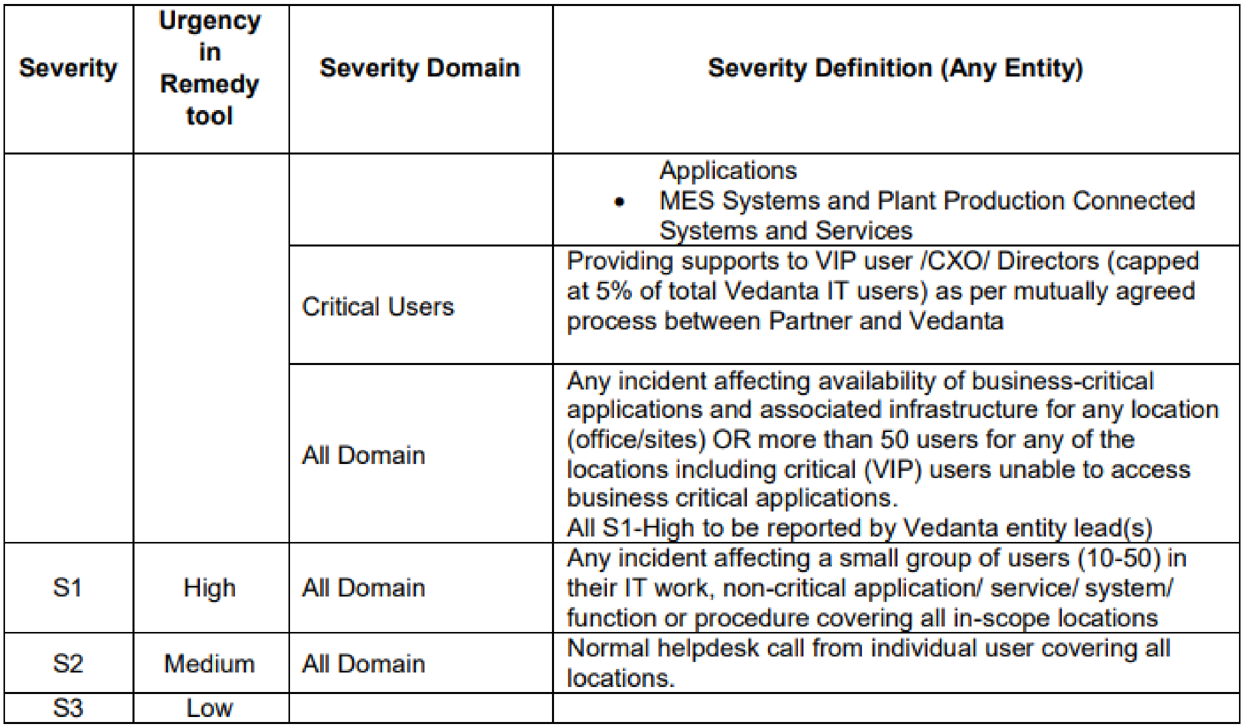
8.5.1 Authority

1. Assist the BC Head in invoking and deactivating the BCP with agreement of CMT.
2. Make recommendations to effectively manage all operational aspects of the plan to the CMT or BC Head.

9. Incident Levels based on Severity



Severity	Urgency in Remedy tool	Severity Domain	Severity Definition (Any Entity)
S1 (Critical)	Critical	SAP	a. Data loss (Prod only), failure of backup restoration (Prod only), SAP instance Server/ OS/ network down. b. Incident related to 'financial accounting closures' during the month end, quarter end and year end. The processes covered are • Financial Closing Process • Payroll Processing • Order to Cash Process • ESS|
		Security	Virus outbreak, data theft, firewall breach, IP theft, Network Security breach.
		Portal	Web application/ web server/ Application server down, Hosting DMZ unavailability, Internal DB server down, router failure, authentication mechanism failure.
		Internet Gateway Services	Internet bandwidth down, router/ proximity server/ switches in internet route/ firewall down, impacting entire business line or core revenue generation process
		Privacy	PII data breach, Lost PII data, violation in accessing the PII data, Inaccurate PII data, Unreasonable storage of PII data.
		Other Applications	• Financial Closing Service and Applications • Sales and Logistics related Service and Applications • Payment and Banking related Services and



Severity	Urgency in Remedy tool	Severity Domain	Severity Definition (Any Entity)
			Applications • MES Systems and Plant Production Connected Systems and Services
		Critical Users	Providing supports to VIP user /CXO/ Directors (capped at 5% of total Vedanta IT users) as per mutually agreed process between Partner and Vedanta
		All Domain	Any incident affecting availability of business-critical applications and associated infrastructure for any location (office/sites) OR more than 50 users for any of the locations including critical (VIP) users unable to access business critical applications. All S1-High to be reported by Vedanta entity lead(s)
S1	High	All Domain	Any incident affecting a small group of users (10-50) in their IT work, non-critical application/ service/ system/ function or procedure covering all in-scope locations
S2	Medium	All Domain	Normal helpdesk call from individual user covering all locations.
S3	Low		

10. Invocation of BCP

If the RTO is missed then the BCP has to be invoked unless deviation is taken.

In addition to the above situations, any incidents which escalate / have the potential to escalate into the "High Impact" category as defined in the *Business Impact Analysis's Classification Matrix* then the BC Head will invoke the Business Continuity Plan on the advice of ITSC/ CMT.

11. Invocation of Crisis

If the incident cannot be managed by the Incident Response Team as per the SLA and the RTO then the following table (Crisis Level Matrix) is to be used for classifying the incident as a crisis. The Crisis Management Plan is invoked by BC Head/CMT in consultation with ITSC.

Level 1	Level 2

The incident affects partially **(damages or makes it inaccessible)** / has the potential to partially affect **(damages or make it inaccessible)** section of the premise where critical IT applications and IT infrastructure are located. The rest of the area is safe for IRT and the affected processes can be re-located to the unaffected areas. E.g., Fire caused partial structural Damage and critical application failure.	The incident completely affects **(damages or makes it inaccessible)**/has the potential to completely affect **(damages or makes it inaccessible)** the premise. For example, a fire has engulfed the entire premise or a virus attack has affected systems at the CMT. Earthquake, fire, or bomb threat causes total structural damage.
The incident has affected critical infrastructure (power failure, hardware failure) making the facility unfit for occupation. **This incident can be resolved within 8 hours.**	The incident has affected critical infrastructure (power failure, hardware failure) making the facility unfit for occupation. **This incident will last for more than a business day/downtime cannot be ascertained**
The incident has affected business at a single location (link failure) system required for carrying out the required activities. **This incident can be resolved within 8 hours.**	The incident has affected business at a single location (link failure) system required for carrying out the required activities. **This incident will last for more than 8 hours/downtime cannot be ascertained.**
The incident has affected less than **50%** of the manpower required for carrying out necessary activities.	The incident has affected **more than 50%** of the manpower required for carrying out necessary activities.

Crisis in which the IRT is not sufficient to handle and CMP has to be invoked	Crisis in which the IRT is not sufficient to handle and CMP has to be invoked and may require assistance from external agencies.

12. Recovery Targets

A Business Impact Analysis (BIA) was carried out to identify the critical IT-applications and maximum acceptable outage (MAO) and recovery time objective (RTO) of every critical application in the data center. A comprehensive BIA exercise had been carried out which included analyzing business processes of Sesa Group data centers, their operational dependencies, resource requirements, technology requirements, impact analysis, and finally RTO values.

The following RTO, MAO values are finalized for the identified critical IT applications after the BIA exercise:

Critical IT Applications – with RTO 8 hours or less.

Application Name	Application Description	RTO	Current MAO	Hosting Location	Priority
SAP - S4HANA	ERP application	30 Min	4 Hrs.	Mumbai DC	1
Microsoft AD	Active Directory	30 Min	4 Hrs..	Panjim DC	2
Microsoft365- On cloud	Email solution	4 Hrs..	8 Hrs..	On Cloud	2
RFID	Weighbridges operation system	4 Hrs..	8 Hrs..	Panjim DC	2
ICICI payment Gateway Application	Payment Gateway Application	8 Hrs..	24 Hrs..	Panjim DC	6
Ariba	Commercial process platform	4 Hrs..	8 Hrs..	On Cloud	2

Application Name	Application Description	RTO	Current MAO	Hosting Location	Priority
Fleet Management system for IOK	Truck trips counting system in mines Counting trips of vehicle	8 Hrs..	24 Hrs..	Panjim DC	6
Microsoft Defender	This application is an anti-virus.	30 Mins	4 Hrs	Panjim DC	
e-Commerce Platform For VAB	Commercial process platform	8 Hrs..	24 Hrs..	On Cloud	6

Please refer Business Impact Analysis Procedure and Consolidated BIA Register for more information.

Significant Applications – with RTO greater than 8 hours and lesser than 24 hours.

Application Name	Application Description	RTO	MAO	Hosting Location	Priority
WMS - Attendance and access	Workforce management Attendance and access control system	24 Hrs.	48 Hrs.	Panjim DC	9
PIM (Privileged Identity Management)	Privileged Identity Management	24 Hrs.	48 Hrs.	Panjim DC	9
MES (Manufacturing Execution System)	Manufacturing Execution System historian and dashboard. Raw material consumption data is provided and pushed to SAP	24 Hrs.	48 Hrs.	Panjim DC-Main Server Local-VAB(Amona)	9
SIEM	Security information and event management system	24 Hrs.	48 Hrs.	Primary- Tata Logger- Panjim DC	9
SAP - Darwin box	HR process automation	24 Hrs.	48 Hrs.	On Cloud	9

Desirable Applications – with RTO greater than 24 hours.

Application Name	Application Description	RTO	MAO	Hosting Location	Priority
SAP - GRC	SAP Governance, Risk, and Compliance	48 Hrs.	72 Hrs.	Mumbai DC	14
SAP - SSO	SAP GUI's **Single Sign**-On Logging in with SSO into all SAP related applications	48 Hrs.	72 Hrs.	Mumbai DC	14
Microsoft EXCHANGE-On Prem	Email solution	48 Hrs.	72 Hrs.	Panjim DC	14

Application Name	Application Description	RTO	MAO	Hosting Location	Priorit y
Microsoft SHAREPOINT	Intranet portal	48 Hrs.	72 Hrs.	Panjim DC	14
FMS (Fuel Management system)	Fuel Management system	48 Hrs.	72 Hrs.	Panjim DC	14
Microsoft - SCCM	Patch management system	48 Hrs.	72 Hrs.	Panjim DC	14
Qlik	Management dashboard system Dashboard shows data of inventory, analytical tool	48 Hrs.	72 Hrs.	Panjim DC	14
HR - PF system	Employee PF system	48 Hrs.	72 Hrs.	Panjim DC	14
Veeam - Server backup	server backup system Backup tool for the servers used	48 Hrs.	72 Hrs.	Panjim DC	14
Commvault - user data backup	user backup system Backup tool for user data	48 Hrs.	72 Hrs.	Panjim DC	14
Forcepoint-DLP	Data Loss prevention system	48 Hrs.	144 Hrs.	Panjim DC	14
Bitlocker - Encryption	HDD encryption	72 Hrs.	1 week	Panjim DC	33
Anti-APT	Anti- advanced persistent threat	48 Hrs.	72 Hrs.	Panjim DC	14
SD - WAN	WAN controls	48 Hrs.	72 Hrs.	Main Controller-Panjim DC	14
Cisco - ICS (centralized wifi solution)	Wifi application	48 Hrs.	72 Hrs.	Main Controller-Panjim DC	14

Application Name	Application Description	RTO	MAO	Hosting Location	Priorit y
Application - eLearning	eLearning application	72 Hrs.	144 Hrs.	Panjim DC	33
Application ISIEP - Business Excellence portal	Business Excellence portal	72 Hrs.	144 Hrs.	Panjim DC	33
Vehicle Uberization for VAB	Vehicle control system	72 Hrs.	144 Hrs.	On Cloud	33
NAC solution	Network access control	48 Hrs.	72 Hrs.	Panjim DC	33
Coal Blend model Application	Coal Blend model Application	48 Hrs.	72 Hrs.	Panjim DC	14
Symphony Tool	IT ticketing tool	48 Hrs.	72 Hrs.	On Cloud	14
VEEAM FACOR – Server Backup	server backup system Backup tool for the servers used	48 Hrs.	72 Hrs.	FACOR CCP DC	14
PRTG	Application is required to uptime of all devices (network, servers, switches, etc.,) by pinging the devices usiing SNMP protocol.	48 Hrs	72 Hrs	FACOR CCP DC	
MVPL Road Dispatch Application	Truck trips counting system from mines to outside. Counting trips of vehicle-tracking the vehicle through GPS (source-destination) for insuring the dispatch outside the facility and creation of delivery order. Time consumed, weighment from RFID weighbridge is also kept.	48 Hrs	72 Hrs	VGCB	

Application Name	Application Description	RTO	MAO	Hosting Location	Priorit y
Control Reporting Tool	SOX control updating tool	48 Hrs.	72 Hrs.	Panjim DC	14

The output of a BIA exercise helps in determining the time objectives for development of suitable recovery strategy. *Please refer to the BIA working sheets for the comprehensive BIA activity and results.*

Please refer to critical IT-Application strategies.

**RTO - Recovery Time Objective,*

**MAO – Maximum Acceptable Outage*

13. Recovery Strategy

After the BIA stage is complete, critical IT-applications are prioritized for recovery. Critical IT-Applications' Recovery strategies are developed to ensure the critical processes/functions are resumed within the agreed Recovery Time Objectives (RTO). Such recovery strategies will also help in reducing the impact on the organization, in the event of any disaster.

Most of the critical IT-applications in Sesa Group have recovery strategies which make them easier to recover from disruption as proactive planning is done to support, in case of a disaster.

It is not practical to develop recovery strategies for each and every business process/function/IT-application, as not all can be recovered, during a disaster, for various business reasons (cost, time required to resume the operations, infrastructure to support the recovery of all processes, etc.).

Hence, strategies are developed only for critical IT-applications where multiple processes are dependent (identified through the BIA Phase) and have a significant impact (operational, financial, legal & regulatory and reputational) on the organization, if not resumed within the agreed time limits.

Below, recovery strategy options are considered for Business Continuity Plan:

Threat Scenario	Possible Threats	Recovery Option
Key Persons not available	**Natural Calamities** **Pandemic** **Poaching by competitor** **Terrorist Attack/Civil Unrest**	● Availability of alternate resources (Backup Plan) ● Multi-skill trained to manage various roles ● Vendor staff availability
Facility (Primary Data Center) not Available. i.e. The threat renders the data center inaccessible. *Note: The disruption is limited to the facility and has not impacted the IT Infrastructure/Connectivity*	**Natural Disasters:** ● Earthquake – No Structural damage but the facility needs to be evacuated for employee safety. ● Water logging making the facility inaccessible **Man-made disasters:** ● Fire – No serious damage but the facility needs to be evacuated for employee safety. ● Vandalism (Worker unrest/Civil unrest) ● Legal or civil action ceasing the license to operate	Since the IT Infrastructure/Connectivity is not affected, BCP will not be required to be invoked. **Option 1:** Critical IT Team members from teams including Application Support, Infrastructure Support and Network support shall gain access and continue operations using one of the following options: ● Work from Home using VPN ● Alternate Sesa Group site **Option 2:** If the above option is not feasible then IT members from the other centers with similar skill sets and necessary access will be required to perform the operations of the members supporting the Primary DC.

IT Infrastructure & Connectivity affected. *<u>Note:</u> This could arise out of threats affecting Information Technology.*	In addition to the threats listed above, the following threats could lead to the said risk Scenarios: Cyber threats including but not limited to: ▪ Cyber Attack ▪ Ransomware / Virus Attack ▪ Denial of Service Attack ▪ Network outage (Vendor end/Fiber cut/key network equipment failure)	**For hardware failure** In case of applications with a DR site the application will be recovered from DR site after recovery using backups. For applications running in HA mode (active – passive) – downtime due to manual changeover. **For application software failure:** OS/ Application it can run through restoration of backup, For Database failure backup restoration option is available.
Information not available	Due to software, hardware failure, natural calamities etc.	1. Documentation of critical activities to be performed (to operate and manage the application). 2. Application installation and configuration guide to be obtained from vendor.
Supplies (Stock) and Utility Services (power, communication link etc.)	Not Applicable	Facility risk assessment done covering: Power supply source, DG set, UPS, Environmental considerations, and network connectivity redundancy tests have already been conducted.

The extent to which strategies and solutions can be implemented will determine strategy selection.

a) Meet the requirements to continue and recover prioritized activities within the identified time frames and agreed capacity.
b) Consider the amount and type of risk the organization may or may not take.
c) Consider associated costs and benefits

14. Business Continuity Strategy

(These plans used for deliberation with function owner / process owner of the identified critical IT-Applications.)

Key Threats

The following threats are considered which could lead to non-availability of key business processes:

- Facility damaged / not accessible
- HO Data Center and Mahape Data center hosting applications affected
- Connectivity between data center and IT-DR site affected.
- Key Persons unavailability
- Vendor Unavailability

14.1. Facility damaged/not accessible

People will Work from Home using VPN connectivity and for Panjim from nearest Sesa Group location.

14.2 HO Data Center and Mahape Data center hosting applications affected

Scenario 1: Data Center -Panjim, Data Center –Mumbai is damaged /is inaccessible.

Description: The incident is location specific and has not affected the immediate area/city in which the facility is located. The employees required to carry out the activities are not affected by the incident.

Possible causes resulting in the threat scenario: fire, explosion, building collapse, blockage of access roads due to flooding/civil unrest, etc.

Business Impact: The activities carried out by the teams will be affected resulting in service delays at the clients' end. Since the availability of services is a key factor for the managed services offering, a disruption would affect the company's reputation.

Recovery Option	Benefits	Challenges
OPTION 1: Application is hosted on Cloud Infrastructure	● The Cloud service provider maintains a minimum Recovery Time Objective (RTO) as geolocation redundancy.	● Will have to make a strategic change as some of the applications do not have Cloud DR e.g., WMS ● Cloud Service Provider's resiliency plans will become key. ● e.g., SAP S4 HANA, SAP Ariba.
OPTION 2: No DR nor Cloud is available	● Rebuild infrastructure. ● Downtime would exceed RTO/MAO. ● System state and database backups will have to be recovered from alternate sites.	● RTO will not be fulfilled ● The Time to recover may be very high. ● Emergency procurement may be more expensive under this extreme scenario where demand may be high. ● System state backup may not be stored at alternate site ● Database backups may not be stored at alternate sites.

Besides the recovery options mentioned above, Sesa Group also has a Cyber Insurance policy.

Scenario 2: Data Center -Panjim, Data Center –Mumbai is available. However, hardware is damaged.

Recovery Option	Benefits	Challenges
OPTION 1: Application is hosted on Cloud Infrastructure	● The Cloud service provider maintains a minimum Recovery Time Objective (RTO) as geolocation redundancy.	● Will have to make a strategic change as the current business model is centralized in nature.

		● Cloud Service Provider's resiliency plans will become key. e.g. SAP Ariba
OPTION 2: Hardware redundancy exists in one site Active- Active mode	● Minimum Recovery Time Objective (RTO) as automatic failover will take place	● Capacity management is crucial to check whether additional capacity requirements can be met.
OPTION 3: Hardware redundancy exists in one site Active- Passive mode	● The Recovery Time Objective will include time for synchronization. ● The Database will be restored from the last available backup.	● Synchronization issues may arise.
OPTION 4: No hardware redundancy exists	● Rebuild infrastructure. ● Downtime may be high as servers will have to be built and system state loaded from backups. ● Database will be restored from backups.	● Time to recover may be very high. ● Emergency procurement may be more expensive under this extreme scenario where demand may be high. ● Where daily backups are done, there may be a loss of 24 hours of data.
	●	●

Scenario 3: Data Center -Goa, Data Center –Mumbai is available. Hardware is available. However, software is damaged

Recovery Option	Benefits	Challenges
OPTION 1: System state backups are available	● The System will be restored using the backup	● Latest version of system state backup may not be available if no backup

	● Time for restoration will be required.	was taken after the change
OPTION 2: System state backups are not available	● Recovery not possible ● Vendor to be contacted	

Scenario 4: Data Center -Panjim, Data Center –Mumbai is available. Hardware is available. Software is available however, database is not available

Recovery Option	Benefits	Challenges
OPTION 1: Database backups are available	● The Database will be restored using the backup. ● Time for restoration will be required.	● If backup frequency is 1 day, 24 hours of data may be lost.
OPTION 2: Database backups are not available	● Recovery not possible	

14.3 Connectivity between Primary data center and IT-DR site affected

Recovery Option when connectivity is lost

Recovery Option
Redundant firewalls and routers exist. Sesa Group has implemented the SD WAN project and legacy MPLS links and ILL are retained as fallbacks. The NOC Team for remote network management monitors the network 24 X7.

14.4 People required to carry out the identified processes are not available

Description: The incident has affected the availability of the people required to carry out the key activities/affected the city, thereby affecting the critical infrastructure like power, transportation, etc.

Possible causes resulting in the threat scenario: Mass casualties or pandemic causing long-term non-availability. Example: Mass attrition, Flooding, Civil Unrest, Terrorist Attack, etc., cause short-term non-availability.

Recovery Option
Critical roles backup plan is formulated.
Multi-skilling with frequent job rotations
All critical IT Infrastructure support has been outsourced to vendors.
Vendor support contract with SLAs to meet Sesa Group’s RTO in place

14.5 Key vendor providing services to critical IT-Application is unavailable.

Description: The incident has affected the availability of the vendor required to carry out the key activities, thereby affecting the critical services/operations.

Possible causes resulting in the threat scenario: Contract with vendor not renewed, Force majeure at vendor.

Business Impact: The activities carried out by the teams will be affected resulting in service delays. Since the availability of services is a key factor, a disaster at the vendor’s end would affect the company’s reputation, incur financial losses and cause operations delays.

Recovery Option	Benefits	Challenges
Option 1: Vendor Redundancy for critical processes that are currently supported by a single vendor, a backup vendor shall be selected to provide a similar service. The redundant vendor	Assured service delivery since in case the primary vendor is unavailable, the secondary vendor will provide the necessary service.	● Increased operational overheads as the in-house team would have to manage two vendors.

will not be prone to the same/similar disasters as the primary vendor.	Reduced dependence on a single service provider.	● A Shortage of vendors providing the required service may force the company to opt for a single vendor.
Option 2: Vendor BCP, the company will include the business continuity clause in its vendor agreement for critical processes that are supported by a single vendor. SOC 1 & SOC 2 reports from vendors are obtained.	Assured service delivery as the vendor will have the capability to deliver the required services even during a disruption at their end.	● Vendor might charge the company for business continuity arrangements that the vendor will put in place to support the company's critical business processes.

15. Invocation of BCP

Task	Responsibility	Done via	Remarks
BC-Plan Invocation Declaration	BC Head in consultation with CMT.	-Telecommunication system -SMS Alerts -Emails	To be done in consultation with the CMT
Necessary action for resumption and recovery at Alternate site	Data Center Head in consultation with Incident Response Team	-Telecommunication system -Emails	To be done in consultation with the BC Head

- All incidents, regardless of severity, should be documented, and reported to the IRT and CMT in order to keep an incident database for future reference.

16. Recovery Back to Normal

Since the BCP scope is IT recovery happens at 100% for all applications as well as IT Infrastructure and upon resumption, recovery will be at normal.

17. Standing Down the BCP

1. The ITSC/CMT will continue to monitor the situation at adequate time intervals (of 2-3 hours each) with inputs from the BC Head and BC Manager to decide whether to continue with the recovery operations or initiate Business Resumption.
2. At any point of time if the CMT/ BC Head feels that the incident is gradually coming under control and the Business Resumption operations can be initiated soon, the BC Manager will inform the respective recovery teams to stand down and prepare for Business Resumption.
3. During this time the recovery teams will ensure the following:

- The ITSC will identify and prioritize processes that needs to be resumed first.
- Critical infrastructure and utilities required to carry out these processes are made available at the primary site.

18. Plan Review

The BC Manager shall review and update this plan annually or if major changes occur in the operations or systems or policy directives by the regulatory authorities.

A. Annexure 1

Business Continuity Plan of Applications:

S.No.	Annexure Name
1.	SAP - S4HANA Business Continuity Plan
2.	O365-On cloud Business Continuity Plan
3.	RFID Business Continuity Plan
4.	ICICI payment Gateway Application Business Continuity Plan
5.	Ariba Business Continuity Plan
6.	Fleet Management Business Continuity Plan
7.	Microsoft AD Business Continuity Plan
8.	e-Commerce Platform for VAB Business Continuity Plan
9.	Microsoft Defender Business Continuity Plan