Risk Management System

(RMS)

Risk Management Policy

Documented information Name: Risk Management Policy

Version No: 2.0

Last Updated: 25 July 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Risk Management Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Incident Management.

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	Incident Management Policy
Documented information Code	SESAIT/ISO31000/Risk Management Policy
Date of Release	25-Aug 22
Documented information Revision	25 Jul 23
Documented information Owner	IT Department
Documented information Author(s)	Pricoris LLP
Documented information Change Reviewer	Dileep Singh – CISO
Checked By	Dileep Singh – CISO
Security Classification	Internal
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature	Date Approved
1	Shobha Raikar (CITO – 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 22	Initial Document		25-Aug 2022
1.1	31-Aug 22	Addition of Risk appetite and addition of IT Aspects after the stage 1 audit	Section 3.2.5	03-Sept 2022
2.0	25 Jul 23	Reviewed with addition of Risk Assessment of PTS systems	Section 8 Annexure 1	10-Aug 2023

Documented information Contact Point

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

Table of Contents

1. Introduction

1.1 Scope

This Policy document is applicable for IT Division of 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, FACOR – Odisha, Sesa Coke - Gujrat and Vazare and VGCB, Visakhapatnam; Nickel Business and Sesa Cement referred as Sesa Group in this document.

1.2 Purpose of the documented information

The objective of this policy is to implement risk management framework and identify risk and opportunities in IT system/applications/process.

1.3 Objective

The objective of this policy is to define the risk management methodology and managing risk to an acceptable level.

2. Policy Statement

Sesa Goa will ensure that proper risk assessment is conducted and the identified risks appropriate risk strategy will be adopted.

Sesa Goa will ensure that IT risk assessment is conducted, and the identified risks appropriate risk strategy will be adopted, wrto organizational operational domains (BCMS, PIMS, ISMS etc), during implementing the same.

3. Guidelines

3.1 Risk Management Methodology

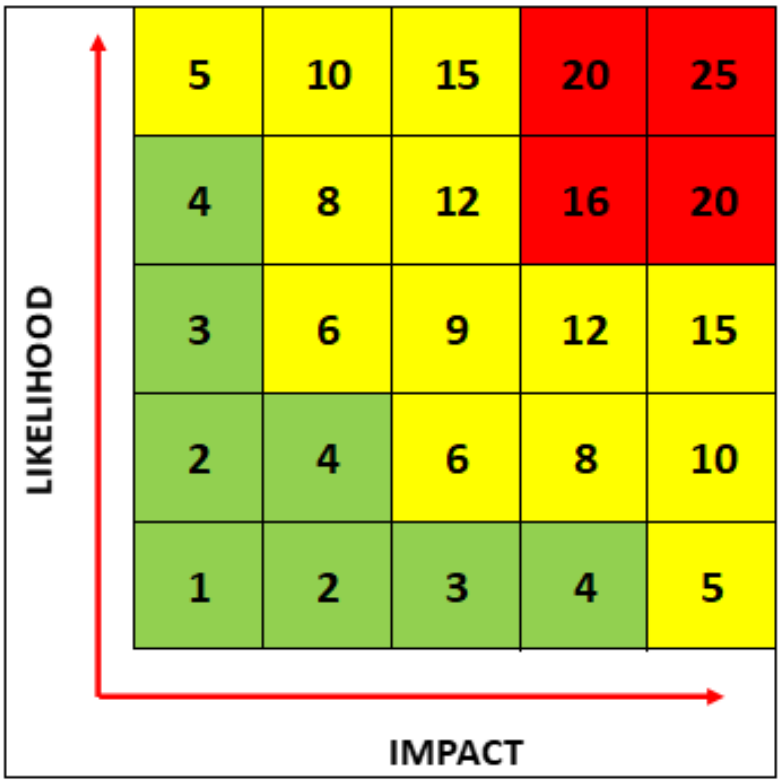
- Sesa Goa should be responsible for developing and maintaining the information risk response criteria to ensure that cost-effective controls and security measures mitigate exposure to risk on a continuing basis. The risk response should identity information risk strategies such as avoidance, reduction, sharing or acceptance.
- Approach of entire risk management program would be consultative in nature. Delphi method would be used to identify, assess & finalize risk & controls.
- CITO would decide acceptability of residual risk.

3.2 Risk Assessment *[1]

- Sesa Goa should ensure that an annual risk assessment is performed or when significant changes occur.
- The scope of the risk management program should be entire Information Technology landscape.
- Sesa Goa should identify the information risks and assign the risk assessment responsibility to relevant information risk owners.
- Sesa Goa should undertake a process-based risk assessment. The scope of the risks shall be IT. This will cover, privacy, continuity, security, governance and strategy, financial risks related to IT.
- Threats will be identified
- Vulnerabilities associated with the threat will be identified
- Risks statement will be articulated.
- Controls will be assessed. based on effectiveness of controls - Refer Annexure 4.1

[1] For Risk Assessment of PTS Systems Refer Annexure 1

- Impact assessment of each & every risk should be done with reference to financial, operational, reputational, Legal & regulatory impacts as per Section 4.3.
- Impact Value = Maximum (Financial, Operational, Legal & Regulatory, Reputational)
- Likelihood of each risk should be assessed as per likelihood considering threat environment refer Section 4.2
- Risk Value = Impact x Likelihood
- Each unique risk generating a risk value basis the above parameters on a scale from 1 to 25
- Risk assessment will be as per risk management framework. Internal audits & assessments like vulnerability assessment, penetration testing, cyber security assessment, SOX process workflow would provide input to risk assessment.
- All the risk identified need to be documented in risk register.
- We would then rate the risk value on a scale of 1 to 25 and achieve the risk rating for individual unique risks. The scale will be as follows:



- **All risks with a value below 5 (Low) will be accepted.**
- Risk owners are identified
- Risk Treatment for risks above the value of 5 will be done. Refer Section below

3.2.1 Risk Treatment:

- Risk treatment shall be as per risk management framework. If required there will be new control so as to lower down the risk rating of existing risk.
- Control should be designed that it should lower down risk to acceptable level.
- If control introduces new risk in environment, these new risks should be captured in risk register.

- Revised Impact and Revised likelihood after the new/ modified control is designed and implemented will be calculated.
- Residual risk will be calculated (Revised Impact * Revised Likelihood)
- If residual risk level is above 15, IT Steering committee will be involved for taking decision of avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk. They will be continuously monitored and reported to the committee.
- For residual risks which continue to be between 5 to 15 - these risks will be discussed for control enhancement. also, insurance/ back-to-back arrangements with vendors if required for risk sharing will be explored through adequate contracting. Further they will be annually evaluated and reported to the senior management.
- If the residual risk level less than 4, the risk will be retained and existing controls will be evaluated based on control self-assessment.
- If the value of Residual Risk is 0 (zero) it does not mean that there is no risk as there is never a zero risk. It only indicates that the risk has controls which have been designed and implemented. Also, we are aware that Controls are subject to internal and external environment and no control can address a risk completely and ensure there will be no error or loss.
- For ease of review, we will categorize residual risks as High, Medium and Low, as follows:

	Residual Risk is High (15and above)
	Residual Risk is Medium (5 and above and below 15)
	Residual is Low (less than 5)

3.2.2 Risk Acceptance:

- Any residual risk post treatment when comes to less than 5 will be considered as acceptable risk.
- Risk register should be signed off by CITO.

3.2.3 Risk Transfer:

- Risk transfer shall be as per risk treatment as per risk framework. Sesa Goa has opted in for cyber insurance program to transfer risk.
- Sesa Goa has transferred some of the risk to vendors by outsourcing some the services.

3.2.4 Risk Avoidance:

- Risk transfer shall be as per risk treatment as per risk framework in case residual risk level is above 15, IT Steering committee will be involved for taking decision of avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk. However, if the management decides to consider the decision towards the risk, continual monitoring and reporting to the board will take place.
- Sesa Goa should document & signoff such risks.

3.2.5 Risk Appetite:

Risks to the values defined for Vedanta are considered in defining the Acceptable Risk.
At Sesa Goa Risk Appetite is defined based on the following principles:

- Entrepreneurship and Innovation involve undertaking risks and the organization will accept risks which are low. Medium risks may be accepted based on factors such as exploiting the risk to create an opportunity, cost benefit analysis etc. All high risks will be treated.
- The organization has zero tolerance for risks to the following values:
- Trust, Integrity, Care, Sustainability and Excellence.
- Risk appetite for IT processes is as follows:
  We accept risks to confidentiality, integrity, availability, privacy and continuity which have a value lower than 5 i.e., low risks (function of impact and probability)
  We have low appetite for risks which are medium risks to confidentiality, integrity, availability, privacy and continuity which are greater than 5 and less than 15 for which treatment plan **may** be prepared and shall be monitored closely.
  We have no appetite for risks which are high risks to confidentiality, integrity, availability, privacy and continuity which are greater than 15 for which treatment plan **must** be prepared and which shall be monitored closely.
  For Business Continuity purposes the risk appetite determines the RTO wherein the impact becomes medium.

3.3 Monitoring

- Risk monitoring will be as per risk management framework.
- Internal & external audits should be conducted to check effectiveness of overall risk management program.
- Test of design should be carried of all controls to check capability of controls created.

4. Annexure:

4.1 Control Effectiveness

Control Rating	Control Effectiveness	Control Description
1	Ineffective	No design of control.
2	Design	Design but not implemented.
3	Design and Implemented	Design Implemented but not operating throughout the year.
4	Effective	Design Implemented and operating effectively throughout the year.
5	Consistently Effective	Design Implemented and operating effectively since last 3 years. No exceptions were identified.

4.2 Risk Likelihood

Risk Likelihood Level		Likelihood Guideline
5	Very High	Likely to occur once in 3-6 months or known incident is last 3-6 months

4	High	Likely to occur within 1 year or known incident in last 1 year
3	Moderate	Likely to occur within 1-3 years or known incident in last 1-3 years
2	Low	Likely to occur within 3-5 years or known incident in last 3-5 years
1	None/Negligible	Likely to occur within 10 years or known incident in last 10 years or has happened in past

4.3 Risk Measurement Matrix

Impact = Average (Financial, Operational, Legal & Regulatory, Reputational)

Impact	Financial*	Operational	Legal & Regulatory	Reputational
Critical (5)	Any single or cumulative potential loss should exceed 20% of company EBITDA or financial and other impacts poses serious threat to the viability of the organization.	Multiple critical applications / services failures across multiple locations leading to complete halt of business or impacting more than 1.2 crore of business loss per hour	Significant breach of contract or rules leading to regulatory censure or action. Action taken against single or multiple persons of the senior management team with heavy penalties. Or Absence / expiry / invalidity / potential for revocation of consent to operate which may impact operations of our major assets / going concern Non compliances which may lead to potential personal liability & prosecution of senior management /Board.	Stakeholders lose trust and faith in management and the organization.
Significant (4)	Any single or cumulative potential loss could range between 10%-20% of EBITDA or financial and other impacts poses serious threat to	Critical application / service failure affecting multiple Operations resulting in serious operational impact or impacting more than .8 crore of business loss per hour	Regulatory or contractual breach resulting in moderate penalties leading to formal enforcement action by the authority or Significant breaches, significant financial penalties & prosecution	Prolonged negative focus and concerns from the stakeholders resulting in serious reputational impact to the organization.

	the viability of the organization.		of staff / stoppage of business. Multiple litigations	
Major (3)	Any single or cumulative potential loss could range between5%-10% of EBITDA or financial and other impacts will materially affect the organization.	Critical application / service failure in a single Operation Sesa Goa resulting in moderate operational impact or impacting more than .5 crore of business loss per hour.	Regulatory or contractual breach resulting in minimal penalty or Negative media coverage / disruption to client / investor confidence on state / national front. Impact on reputation of company. Public exposure in national media.	Negative media focus and concerns from stakeholders resulting in minimum reputational impact to the organization.
Moderate (2)	Any single or cumulative potential loss could range between 2%-5% of EBITDA or financial and other impacts will not materially affect the organization.	Any single or cumulative potential loss could range between .5 crore to .024 crore per hour or financial and other impacts will not materially affect the organization.	Trigger of regulatory or contractual obligations resulting in receiving notice and subsequent process.	Short term anonymous rumours in local media at any location with negligible impact to the organization.
Manageable (1)	Any single or cumulative potential loss that will have no or less than 2%-of EBITDA of financial impact on the organization	Service failure for a single user of Sesa Goa resulting in no Operational impact or loss could range less than .024 crore per hour or financial and other impacts will not material.	No legal or regulatory impact to the organization	No reputational impact to the organization

*Financial Figures are judgmental & vary from risk to risk.

5. Enforcement

Any employee found to have violated this policy may be subject to revocation of access and disciplinary action.

6. Responsibilities

- CITO is responsible for ensuring the following:
    - Implementation of policy and ensuring compliance.
    - Ensuring development of underlying standards, procedures and roles of managing risks.
- The CISO along with risk owner shall ensure enforcement, effectiveness, monitoring and reporting.

7. Definitions and List of Abbreviations

Term	Definition
Framework	Sets an overall approach to managing certain areas of the business. They help outline guiding principles and key standards to influence decision making in line with the organization's strategy and objectives.
Guidelines	Guidelines are recommendations to enable employees to perform their general responsibilities or specific tasks effectively. Conformance is expected unless, when applying professional judgement, circumstances justify deviation
Regulations	Regulations, legislations and standards that govern the conduct and management of company. References to regulations should be reviewed regularly to ensure they are correct and accurately reflect company regulatory obligations.
IT Risk	IT business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within Sesa Goa.
Risk management	Coordinated activities to direct and control an organization with regard to risk
Risk management policy	Statement of the overall intentions and direction of an organization related to risk management
Risk management framework	Risk management framework is the scheme specifying the approach, the management components and resources to be applied to the management of risk
Risk management process as defined in Framework	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.

8. Annexure 1 Risk Assessment for PTS systems

The methodology for Risk Assessment for SCADA systems is based on NIST 800-82 and controls are mapped to ISO 27001:2013.

Risk Impact Rating	Effectiveness	Impact
3	High	Risks categorized as high impact have significant adverse consequences on the organization and its SCADA systems. The impact may include substantial financial loss, prolonged disruption of critical operations, severe reputational damage, or serious regulatory non-compliance. These risks pose a significant threat to the organization's ability to achieve its objectives and may require additional resources, measures, or contingency plans to mitigate effectively.
2	Medium	Risks categorized as medium impact can have moderate adverse consequences on the organization and its SCADA systems. The impact may include moderate financial loss, temporary disruption of critical operations, moderate reputational damage, or non-compliance with significant regulatory requirements. These risks may have a noticeable effect on the organization's ability to achieve its objectives but are still manageable within existing resources and capabilities.
1	Low	Risks categorized as low impact typically have minimal adverse consequences on the organization and its SCADA systems. The impact may include limited financial loss, temporary disruption of non-critical operations, minor reputational damage, or minimal regulatory non-compliance. These risks may have a limited effect on the organization's ability to achieve its objectives.

Risk Impact = Maximum (Confidentiality Impact, Integrity Impact, Availability Impact)

Rating		Likelihood Criteria
High	**3**	Likely to occur once in 3-6 months or known incident is last 3-6 months
Medium	**2**	Likely to occur within 6 months-2 years or known incident in last 6 months-2 years
Low	**1**	Likely to occur within 5 years or known incident in last 5 years

Risk Value= Impact Value x Likelihood

Risk Rating	Risk Type	Value Range
1	Low	1 to 3
2	Medium	4 to 6
3	High	7 to 9

For PTS systems low Risk Appetite for risks which are medium risks to confidentiality, integrity, availability, which are greater than 3 and less than 6 for which treatment plan **may** be prepared and shall be monitored closely.

We have no appetite for risks which are high risks to confidentiality, integrity, availability, which are greater than 6 for which treatment plan **must** be prepared and which shall be monitored closely.