vedanta | sesa goa iron ore

Risk Management System

(RMS)

Risk Management Framework

Documented information Name: Risk Management Framework

Version No: 2.0

Last Updated: 25th July 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Risk Management Framework

Abstract: This Documented information is a procedure Documented information highlighting the Risk Management Framework

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 framework
Date of Release	25-Aug 22
Documented information Revision	25 July 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 2022	Initial Document		25 Aug 2022
1.1	31-Aug 2022	Changed version control as per stage 1 audit		03 Sept 2022
2.0	25-Jul-2023	Review	Section 2 added Risk Appetite for PTS. Added Annexure 2 for PTS Risk Assessment methodology.	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. Sesa Goa Vision

Be the highest value creator in the iron ore industry contributing to the growth of the nation. IT is the enabler for achieving the vision.

2. Sesa Goa Values

- **Entrepreneurship**

People are our most important assets; they are at the heart of everything we do. We dedicatedly create an enabling environment to support them in pursuing personal and professional goals.

- **Excellence**
  Our primary focus is delivering value of the highest standard. We are constantly looking at ways to reduce costs and increase production in our businesses through benchmarking best practices and employee participation.
- **Trust**
  We actively foster a culture of transparency in our interactions and encourage an open dialogue which ensures mutual trust and respect.

- **Sustainability**
  We practice sustainability within the framework of well-defined governance structures and policies and with the demonstrated commitment of our management and employees. We aim not only to minimize damage to the environment from our project but to make a net positive impact on the environment where we work.

- **Innovation**
  We encourage innovation that leads to zero harm, zero waste and zero discharge environment and optimal utilization of natural resources, improved efficiencies and recoveries of by-products.

- **Integrity**
  We engage ethically and transparently with all our stakeholders, taking accountability of our actions. We maintain highest standards of professionalism and stringently comply with international policies and procedures.

- **Care**
  We are committed to our triple bottom line of 'People, Planet and Prosperity' to create a sustainable future in a "zero-harm, zero waste and zero discharge" environment for our communities.

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:

1. 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.
2. 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 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.

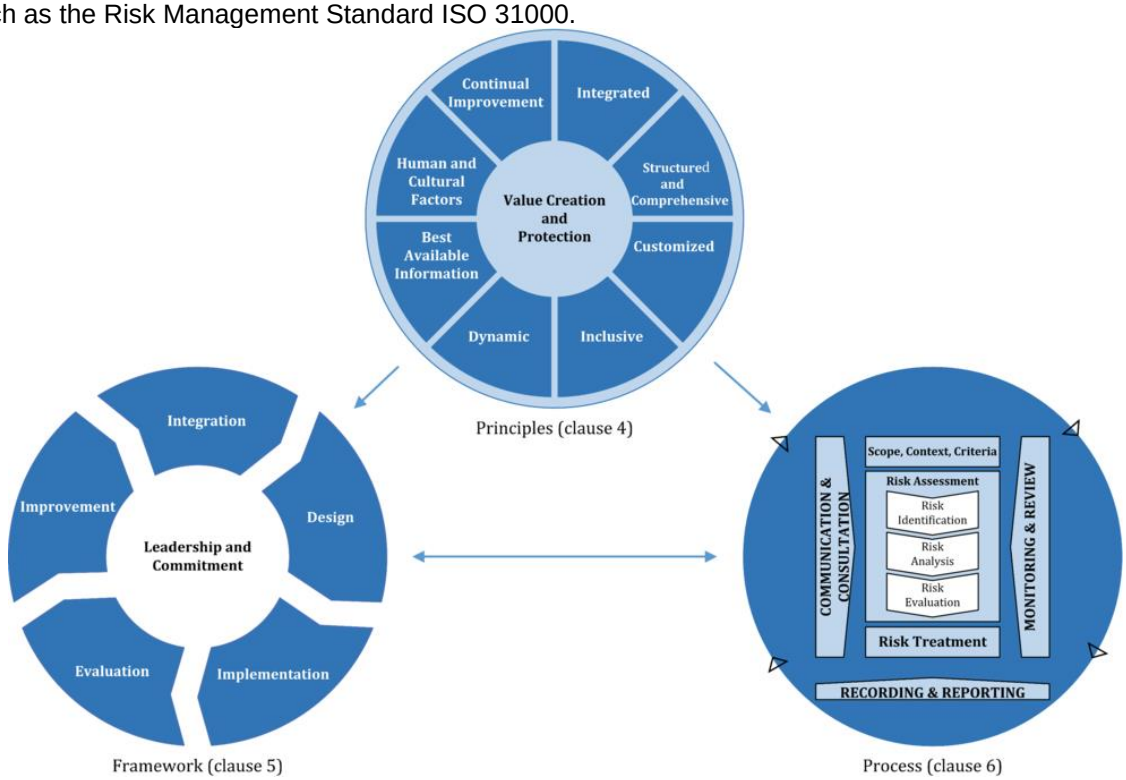
We have no appetite for risks which are high risks to confidentiality, integrity, availability, which are greater than 6 for which treatment plan **must** be prepared and which shall be monitored closely.

3. Framework for IT ERM at Sesa Goa

The Organization is committed to high standards of business conduct and good risk management to:

- Protect the Organization's IT assets and information;
- Achieve Quality Services, Privacy, Information Security & Business Continuity overall objectives, in a pro-active manner through Risk Management;
- Achieve sustainable business growth supported by IT;
- Timely Corrective Actions for Incidents & through Risk Management try to avoid major surprises related to the overall control environment;
- Take appropriate risk strategy towards IT decisions in line with business decisions requirements
- Safeguard shareholder investment and with vision of societal benefits;
- Ensure compliance with applicable legal requirements (statutory and regulatory) apart from the adopted management system standards;

This Framework is intended to ensure that an effective risk management framework is established and implemented within the Organization covering IT and to provide regular reports on the performance of that framework, including any exceptions, to the CITO and if required to CEO having representation in Board of Directors of the Organization. This Risk Management framework and policy complements and does not replace other existing compliance programs. This document is built on the established principles of sound risk management as detailed in recognized sources such as the Risk Management Standard ISO 31000.



3.1 Applicability

This Risk Management Framework 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, Sesa Coke, FACOR – Odisha, Gujrat NRE and VGCB, Visakhapatnam; Nickel Business and Sesa Cement referred as Sesa Group in this document.

This framework provides a common approach to managing any type of IT risk. It will be used to conduct any significant activity, including important decision-making at all levels of IT.

3.2 Risk Management Objectives

The objective of Risk Management is to help managers make informed actions which:

- Provide a sound basis for integrated IT enterprise-wide risk management as a component of good corporate governance.
- Improve business aligned IT performance by informing and improving decision making and planning.
- Promote a more innovative, risk awareness culture in pursuit of opportunities to benefit the organization.

To realize the risk management objective, the Organization aims to ensure that:

- The identification and management of IT risk is integrated in the day-to-day management of the business
- Risks are identified, assessed in the context of Organization's appetite for IT risks and their potential impact on the achievement of objectives, continuously monitored and managed to an acceptable level
- The escalation of risk information is timely, accurate and gives complete information on the risks to support decision making at all management levels.

3.3 Risk Management 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 organisational operational domains (BCMS, PIMS, ISMS etc), during implementing the same.

Principles

The principles contained in this framework will be applied across IT function of the principles outlined in this framework provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. These principles are the foundation for managing risk in Sesa Goa and are considered during establishing the organization's risk management framework and processes. These principles enable the organization to manage the effects of uncertainty on its objectives and create and protect value.

For effective risk management following principles are adopted at Sesa Goa:

Integrated

Risk management is an integral part of all organizational activities' IT function. Sesa Goa will adopt an integrated risk management approach covering all the risk domains affecting IT including security, privacy and continuity risks and mapping them to common controls which can address multiple requirements in an integrated manner.

Structured and comprehensive

A structured and comprehensive approach to risk management contributes to consistent and comparable results. The IT risk process will be structured by following a well-defined methodology and comprehensively considering all risks such as risks related to information security, privacy, business continuity, quality of IT services, IT environmental risks, IT health & safety (including people risks), IT operational, IT strategy and IT Financial risks.

Customized

The IT risk management framework and process are customized as per organization risk appetite and management culture and style and proportionate to the organization's external and internal context related to its objectives. For Business Continuity purposes the risk appetite determines the RTO wherein the impact becomes medium.

Inclusive

Appropriate and timely involvement of all stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management. In order to make the culture inclusive in IT Department awareness training will be provided.

Dynamic

IT Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner. Risk identification and profiling will be a annually exercise to capture emerging IT risks in a timely manner.

Best available information

The inputs to IT risk management are based on historical and current information, especially the identification, analysis (likelihood and impact) of risks which consider current as well as on future expectations. Additionally, IT Department will ensure that the information used in Risk Assessment is with 100% Integrity (Accurate & Complete)

Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

Human and cultural factors

Human behaviour and culture (of IT Department – its employees, partner and vendor employees) significantly influence all aspects of risk management at each level and stage.

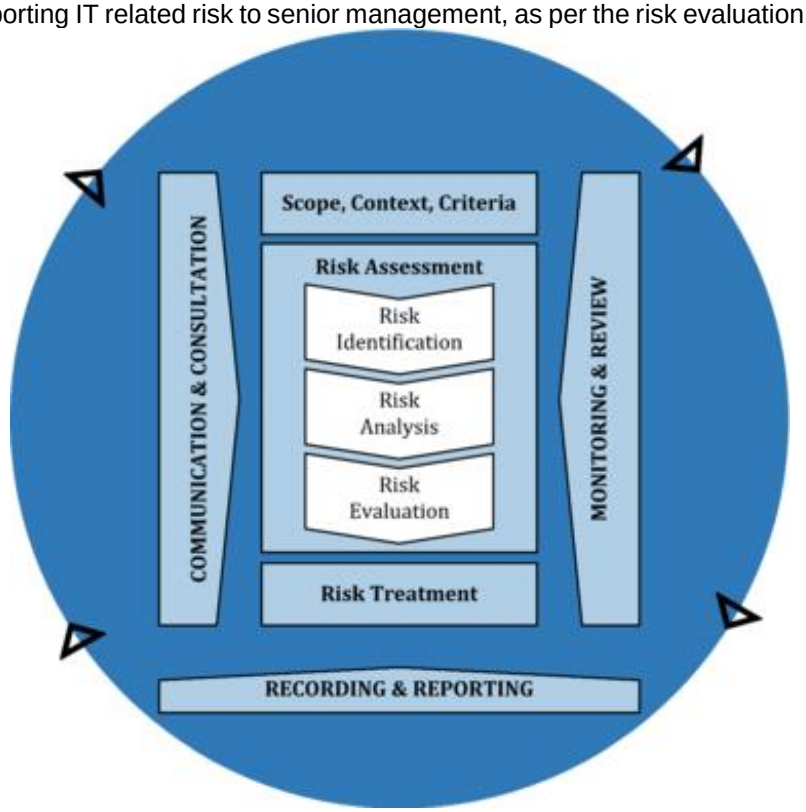
Continual improvement

Risk management is continually improved through learning and experience.

4. Risk Management Process

4.1 General

The IT risk management process at Sesa Goa involves the systematic application of policies and practices to the activities of communicating and consulting (top-down as well as bottom-up approach). Sesa Goa aims at establishing the context and assessing, treating, monitoring, reviewing, recording and reporting IT related risk to senior management, as per the risk evaluation based on the risk appetite.



The risk management process is an integral part of Sesa Goa IT management and decision-making. This process is integrated into the structure, operations and practices of Sesa Goa risk management. It can be applied at strategic, operational, program or project levels.
The risk management process within Sesa Goa is customized to achieve business objectives and to suit the external and internal context in which Sesa Goa operates.
The dynamic and variable nature of human behaviour and culture is considered throughout the risk management process.
The risk management process is sequential as well as iterative.
The framework is designed to ensure communication and consultation of risk for adequate management. It is designed to assist relevant stakeholders understand risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk.

It involves consultation by obtaining feedback and information to support decision-making. Close coordination between communication and consultation facilitates factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals. For internal and external context refer document Context of Organization.

4.2 Risk Criteria

Sesa Goa has defined risk categories, area and risk measurement matrix, clearly laying down the amount and type of risk that it may or may not take, relative to its objectives. Sesa Goa has also defined criteria to evaluate the significance of risk and to support decision-making processes.
For Risk Category refer Annexure I: List of risk categories and areas.
For Risk Measurement refer Annexure VI: Risk Measurement Matrix.

For risk criteria the following approach would be taken to align with the organization's values, objectives and resources and aims to be consistent with policies about risk management. The criteria are defined taking into consideration the organization's obligations and the views of stakeholders.

It is established and followed for the risk assessment process which is dynamic and continually reviewed and amended, if necessary. For PTS Risk Assessment methodology refer Annexure 1.1.

To set risk criteria, the following is considered:

- The impact covering nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible) and consequences (both positive and negative)
- Likelihood will be defined and measured;
- In risk criteria we will use consistency in the use of measurements and have a communicating and consultive approach to determine the level of risk based on risk measurement matrix which shall guide on the level of risk and ensure we have combination and sequences of multiple risk taken into consideration;

1. The risk would be assessed for Information technology.
3. Threats will be identified
4. Vulnerabilities associated with the threat will be identified
5. Risks statement will be articulated.
6. Controls implemented will be identified
7. The risk assessment will help to identify appropriate controls. In order to do so the risk assessment for IT shall consider the following attributes:
    - **Control Types**: It takes the perspective of when and how the control impacts the risk outcome during an incident. These attribute values consist of:

      These can be used to check if adequate controls to detect events into place—not just those to prevent incidents.
    - **Information Security and Privacy Properties**: This takes the perspective of which characteristic of information the control will contribute to preserving. Attribute values consist of:

        - Privacy
        - Confidentiality
        - Integrity; and
        - Availability.

      Commonly referred to as "CIAP," this attribute can be very helpful during the risk assessment process since considering mitigation of risks associated with CIA is one of the requirements of ISMS clause 6.1.2 within ISO 27001

- **Operational Capabilities:** This takes a practitioner's perspective of capabilities. IT helps assign a risk or associated control to the responsible departments. There are several possible attribute values, which include but are not limited to:

    - Governance.

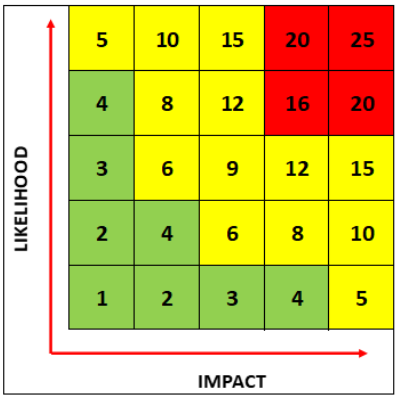
- Asset Management.
- Information Protection.
- Human Resource Security; and
- Physical Security, etc.

This group helps in delineating or assigning risk/control ownership.

- **Cyber Security Domains**: Information Technology also includes the cyber domain, this attribute aligns controls to the well-known NIST Framework.
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

- Security Domains: It takes the perspective of information security fields, expertise, services, and products. Attribute values consist of:
  - Governance and Ecosystem.
  - Protection (including Data Protection)
  - Defence; and
  - Resilience.

2. Impact assessment of each & every risk should be done with reference to financial, operational, reputational, Legal & regulatory impacts. Refer Annexure VI.
   Impact Value = Maximum (Financial, Operational, Legal & Regulatory, Reputational)
   This is done at two stages – First, after listing all Existing Controls for Vulnerabilities and Second after Listing Mitigation controls for Vulnerabilities.
3. Likelihood assessment of each and every risk should be done as per Annexure VI.
4. Each unique risk would be generating a risk value basis the parameters as per Annexure VI on a scale from 1 to 5.
5. Risk Value = Impact x Likelihood
6. Each unique risk generating a risk value basis the above parameters on a scale from 1 to 25.
7. We would then 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:



1. All risks with a value below 5 (Low) will be accepted – considered as Normal Incident – but treated if need be if Impacts are more than risk appetite which are against the values of Sesa Goa;
2. All risks with value between 5 to 15 can be called as medium and require risk reduction treatment control to bring down to Low;
3. All risks with value > 15 may be treated as high and require risk reduction control treatment to bring down to Low;

The interpretation of Likelihood & Severity of Impacts in each Operational Domain be considered as:
Information Security (ISO 27001), PIMS (ISO 27701) and BCMS (ISO 22301)
The Likelihood of Impact only changes or reduces, due to any mitigations which is preventive in nature e.g. Threat Intelligence
The Impact can be reduced if the mitigation is corrective or detective in nature e.g. incident management

Risk Assessment

4.2.1General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment will be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It will use the best available information, supplemented by further enquiry as necessary.

4.2.2Risk Identification

Comprehensive risk identification using a well-structured systematic process is critical, because a potential risk not identified is excluded from further analysis. Identification should include all risks whether or not they are under the control of the Organization. Risks can be identified in a number of ways, viz.:

- Structured discussion and workshops;
- Brainstorming sessions;
- Occurrence of a loss event;
- Review of documents.
- Results of vulnerability assessments and penetration testing

Sesa Goa has adopted structured discussions and consultive approach for the identification of risks. During the discussions following illustrative factors and relationship between these factors, should be considered:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;
- time-related factors;
- biases, assumptions and beliefs of those involved.

All the above factors are largely qualitative in nature and hence Sesa Goa has developed IT Steering committee to brainstorm and arrive on decision for the same. The final decision on the same will be reviewed by the CITO.

Each Risk Owner must periodically review the risks within their risk areas. This review should include identification for all significant functional areas. Discussion and consultive approach or brainstorming sessions may be conducted amongst the focus groups to identify new risks that may have emerged over a period of time.

All identified risks should be updated in a risk register. Risk registers should be periodically reviewed by the respective risk owners to ensure pertinence of the risks listed. Risks that would have ceased should also be closed appropriately. The CISO should ensure that the risk register is reviewed and updated annually.

4.2.3Risk Analysis

All the processes will be risk assessed. All risks which are in category of high or medium will be risk treated. The risks will be assessed on qualitative three-fold criteria.

The three components of risk assessment are:

- Control effectiveness
- Likelihood of occurrence of the risk event,
- Magnitude of Impact if the risk event occurs, and

The time related factors and volatility, complexity, and inter-relationship of risk (financial, operational, legal & regulatory and reputational) will be considered while giving impact rating. The combination of control effectiveness, likelihood of occurrence and the magnitude of impact provides the risk level. The likelihood and impact should be rated over a period of 12 to 18 months. Guidance as provided in Annexure VI – Risk Measurement Matrix may be used for this qualitative assessment.
In determining what constitutes a given level of risk the following scale is to be used for determining control effectiveness:

Control Type	Status	Residual Risk Status
Risk Reduction Controls from Annex A or Self Designed	Partially Implemented	Medium – Not Acceptable – monitored closely with more frequency
	Fully Implemented	Low – Acceptable – Less monitored
Risk Monitoring Controls requiring Human Intervention for Control Enforcement / Corrective Actions	Human Monitoring	Medium – Not Acceptable – monitored closely with more frequency
	Electronic / Auto Allert Systems	Low – Acceptable – Less monitored

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.

In determining what constitutes a given level of risk refer to the likelihood scale given in annexure VI.

Refer Annexure VI for impact assessment guidance. Qualitative approach is taken for risk assessment since precise quantification of the INR value impact of IT risks is sometimes impractical, since the ultimate cost would depend on a significant number of variables. Ultimately, Risk analysis will provide an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

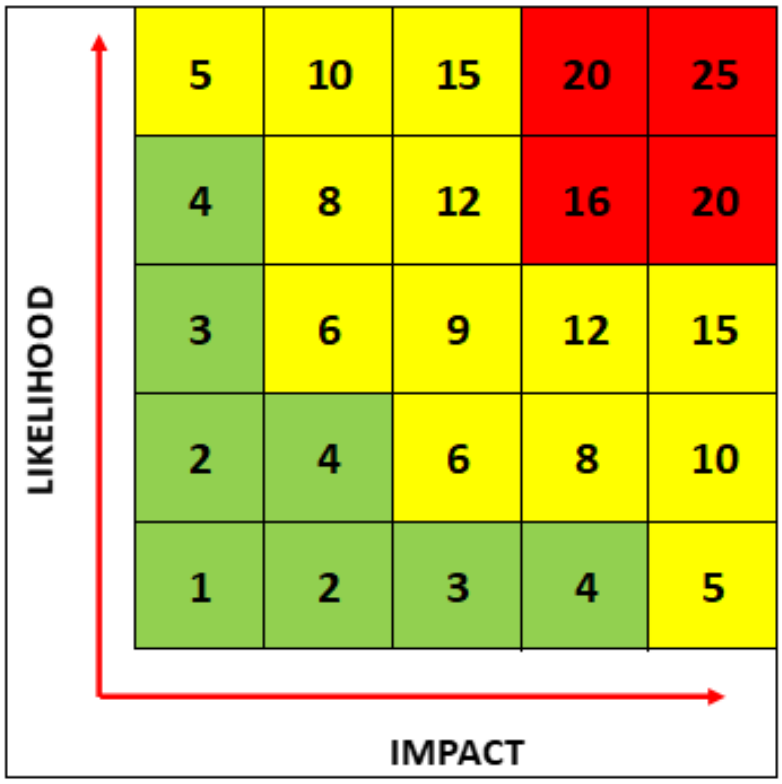
The magnitude of impact of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls. Impact and likelihood may be determined qualitatively, since IT risks are not measurable in exact values

being pervasive and judgmental in nature. Further, in many cases they are emerging risk where no past data are available, subjective estimates may be made which reflect an employee's or group's degree of belief that a particular event or outcome will occur.

4.2.4Risk Evaluation

Impact and likelihood are combined to produce a level of risk and rated on a scale of 1 - 5. The risk should be classified into 3 zones based on the combined scores of the risk.

- Risks that score within a red zone are considered High and require immediate action plans to address the risk with adequate risk treatment options.
- Risks that score within the yellow zone are considered Medium where action steps to maintain the existing control and if required develop or enhance existing controls if needed.
- Risks that score within the green zone are considered Low or in control and nothing more is required to be done.



- Risk is assigned rating 1-3 on Impact and likelihood Risks are moderated as follows:

Normalized Risk Rating	Risk Type	Value Range
1	Low	0 to 4
2	Medium	5 to 15
3	High	16 to 25

The objective is to define risk treatment and monitoring strategies for all risks evaluated to ensure appropriate attention and effective utilization of Organization's resources in managing these risks.

The output of a risk evaluation is a prioritized list of risks for further action. This should be documented in a Annually Risk Management Report refer Annexure 5.

4.2.5Risk Treatment/ Action Plan

Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Treatment options may include:

- Accepting the risk level within established criteria;
- Transferring the risk to other parties viz. insurance;
- Taking or increasing the risk in order to pursue an opportunity and thus, retaining the risk by taking informed decision.
- Avoiding the risk by hedging / adopting safer practices or policies; and
- Reducing the likelihood of occurrence and/or consequence of a risk event by defining risk controls. In practice generally IT will define policies and procedures and implement controls for all risk which are rated in red zone (significant and critical).

The approach for the same will as follows:

- The controls need to be identified by the risk owner to address the risk or alternatively decision has to be taken along with CITO for any other alternate mechanism as mentioned above.
- The controls owner needs to clearly define the control type and the control frequency.
- The control types can be as follow:
  - Preventive - which prevents the risk event form happening, or
  - Detective – they detect the risk on timely basis and are intended to reduce the risk.
  - Corrective – they correct the risk and ensure continual improvement e.g. lessons learnt
- For each unique risk there can be multiple controls and each control given a rating as per the criteria above.
- If control introduces new risk in environment, these new risks should be captured in risk register.
- Risk treatment will be done only if the residual risk is Medium or high.
- Residual Risk (after implementing/modifying additional control) = 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 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.
  - Any residual risk post treatment when comes to less than 4 it will be considered as acceptable risk.

- Risk transfer shall be as per risk treatment as per risk framework. Sesa Goa may opt in to for cyber insurance program or outsourcing with back-to-back arrangement to transfer risk.

- For ease of review, we will categorize residual risks as High, Medium and Low, as follows:

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

The residual risk assessed is in category of Medium or above it should be profiled in the 'Risk profile format' in Annexure IV. The profile contains details of the risk, its impact, likelihood, risk value, controls documentation and specific and practical action plans etc. Action plans need to be time bound and responsibility driven to facilitate future status monitoring. Mitigating practices and controls shall include determining policies, procedures, practices and processes in place that will ensure that existing level of risks are brought down to an acceptable level. In many cases significant risk may still exist after mitigation of the risk level through the risk treatment process. These residual risks will need to be considered appropriately.

4.2.6 Risk Acceptance:

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

4.2.7 Risk Transfer:

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

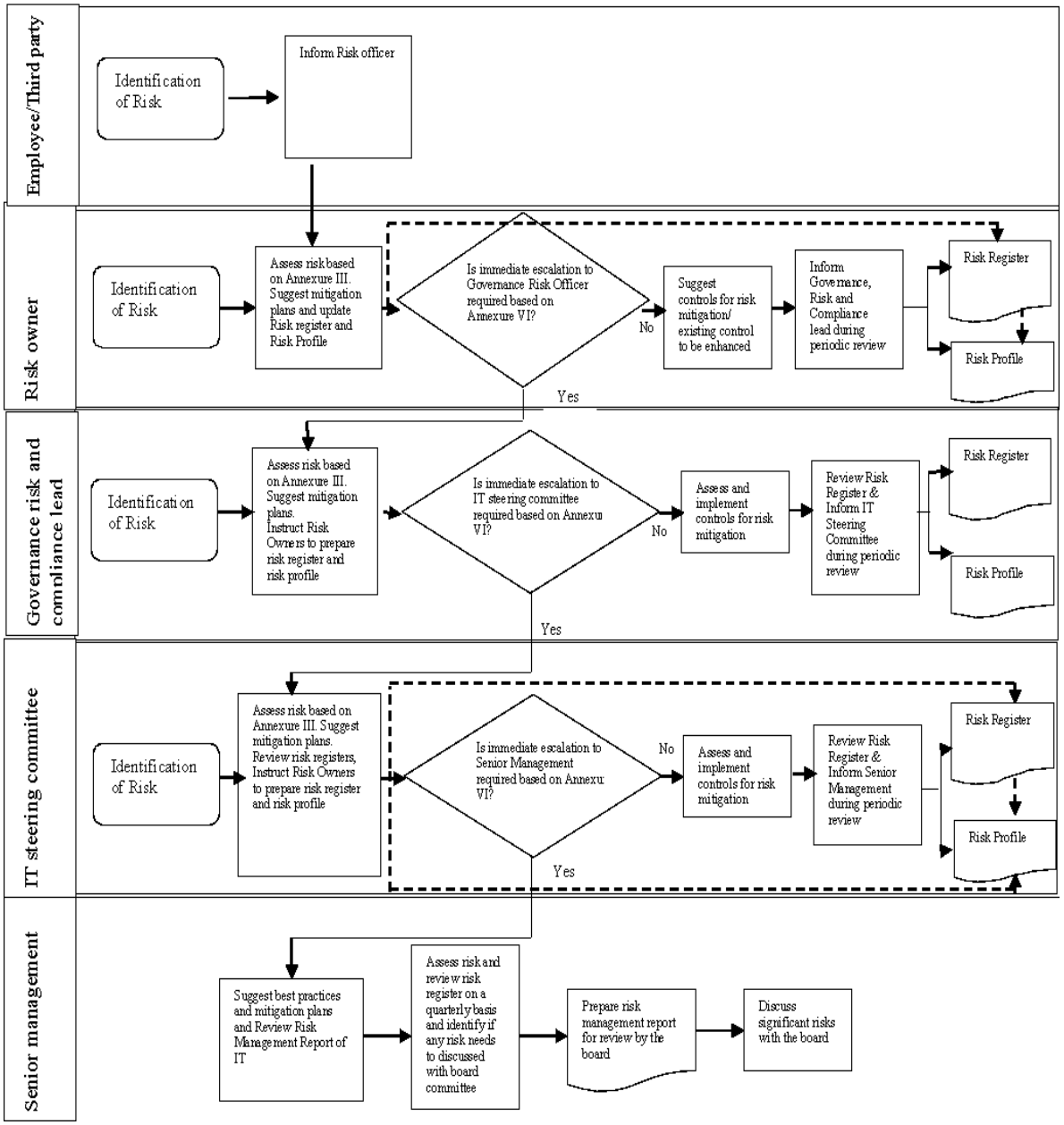
4.2.8 Risk Avoidance:

- 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 what all the risk which need to avoid.

4.2.9 Escalation of Risks

It is critical to institute an effective system of escalation which ensures that specific issues are promptly communicated and followed up appropriately. Every employee of the Organization has responsibility of identifying and escalating the risks to appropriate levels within the organization. The respective risk owner and the CISO will determine whether the risk needs immediate escalation to next level or it can wait till subsequent periodic review. Overall escalation and information flow within the Organization will be as follows:

Process of Escalation of Risk across Organization levels



4.2.10 Risk Reviews

Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities. Few risks remain static. Ongoing review is essential to ensure that the management plans remain relevant. Factors, which may affect the likelihood and impact of an outcome, may change, as may the factors, which affect the suitability or cost of the various treatment options.

A risk review involves re-examination of all risks recorded in the risk register and risk profiles to ensure that the current assessments remain valid. Review also aims at assessing the progress of risk treatment action plans. Risk reviews should form part of agenda for every IT

steering annually meeting. The risk register should be reviewed, assessed and updated on a annually basis.

The CISO is responsible for ensuring that the is reviewed and updated at least annually.

4.2.11 Structure

The Risk Management Structure, roles and responsibilities are set out in Section 5.

4.2.12 Risk Management Approach

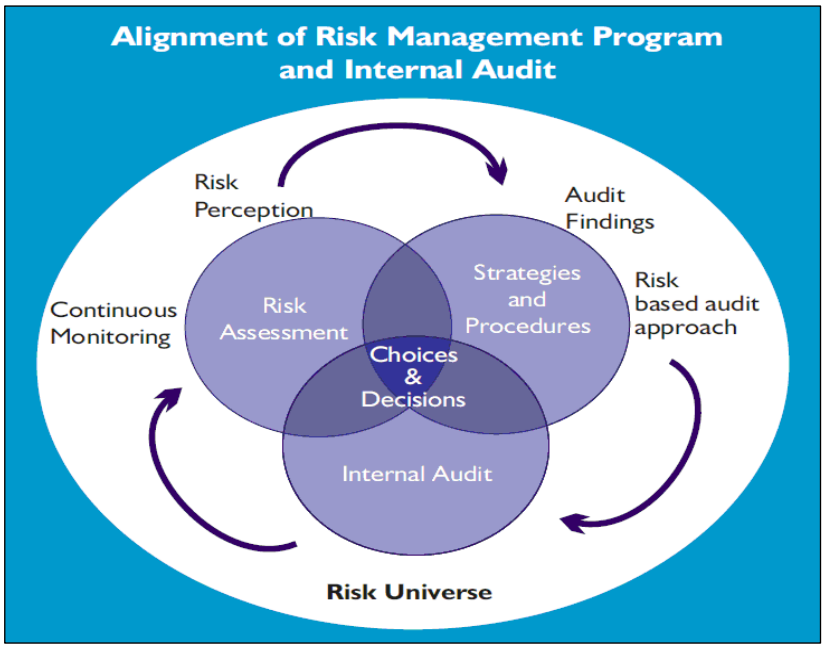
The Risk Management Approach is explained in detail in Section 4.

4.2.13 Internal Audit

The Organization recognizes the synergy and inter-dependence between internal audit and risk management program and wishes to draw up a plan which will ensure that:

- Internal Audit provides effective, independent and objective evaluation of risk management process at regular intervals.
- Internal Audit draws its plans based on outcomes of risk assessment program.
- Risk management program receives constant inputs on controls evaluation from the internal audit.
- Structured approach and mechanism are followed.

Relationship of Risk Management with Internal Audit is given in the figure below:



Internal Audit and Control Self-Assessment (CSA) will be done every year to review the IT risk management process to assure and review the quality and effectiveness of process design, implementation and outcomes. Annually meeting review of the risk management process and its outcomes would be a done by the IT steering committee, CISO will coordinate and provide relevant inputs necessary for the purpose of the meeting.

Any residual risk greater than 4 shall be subject to internal audit and at least annually. Further, risk treatment plans shall be subject to internal audit annually so as to review if the control has been designed, implemented and operating effectively and residual risk has been brought to an acceptable level.

4.2.14 Documentation

Appropriate documentation of each stage of the risk management process should be followed. This framework provides a guide to documentation standards and how they are to be utilized.

The documentation will serve following purposes:

- Demonstrate that the risk management process is conducted properly;
- Provide evidence of a systematic approach to risk identification and analysis
- Provide a record of risks to support the development of a database of the Organization's risks;
- Provide responsible management with risk treatment plans for approval and subsequent implementation for those risks with a residual risk rating in excess of risk tolerance limits;
- Provide accountability for managing the risks identified;
- Facilitate continuous monitoring and review;
- Share and communicate risk management information across the Organization.

The responsibility for documenting the individual risks has been assigned to the risk owners. Business units are responsible for performing and documenting risk assessments and developing appropriate treatment plans.

The key documents pertaining to the risk management process that needs to be maintained by the Organization are:

- Risk Management Framework and Policies
- Risk Register: It contains list of all risks that have been identified during the periodical review. It is the key document used to communicate the risk assessment and current status of all known risks and is used for management control, reporting and reviews. The consolidated risk register is owned by IT Steering Committee and will be maintained by the CISO with support of respective risk coordinators. A template of the risk register is given as Annexure-II. Risk registers indicating the risks identified during the brainstorming sessions/ interviews for the Sesa Goa IT functions have already been discussed.
- Risk Assessment Template: This template contains details of the risk scores for each of the identified new risk presented to the IT steering committee. A copy of the template is given as Annexure-III.
- Risk Profile: The key risk identified should be profiled. The risk profile details the attributes of risk and the response to determine how each risk will be treated. A Template is given as Annexure-IV.
- Annually Risk Management Report: The report is to be placed before the IT steering committee for review and approval. A template is given as Annexure V.

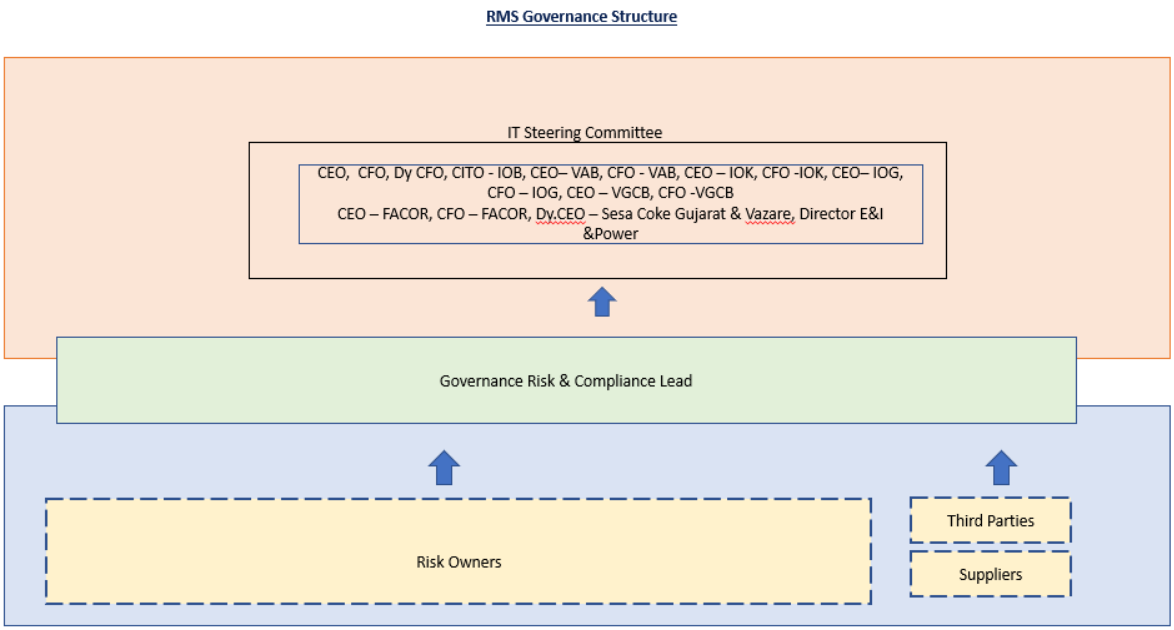
4.2.15 Reporting

A 'Risk Management Report' should be prepared by the CISO and signed by CITO and discussed by the IT Steering Committee.

The frequency of review and reporting of the risk management is given below:

Function	Frequency	Template Annexure reference	Date
Establishment of Risk Management Process	Yearly		As approved
Risk register	As and when risk is identified and assessed, at least once annually	Annexure II	July
Risk assessment	As and when risk is identified, at least once annually	Annexure III	July
Risk profile	Annually	Annexure IV	December
Risk Management Report	Annually	Annexure V	December
Internal Audit	Annually	N/A	July
Control Self Assessment	Yearly	N/A	July

5. IT Enterprise Risk Management Organization



5.1 IT Steering Committee

5.1.1Membership

Members of the IT steering committee will consist of the following members:

CEO,
CFO,
Dy CFO,
CITO - IOB,
CEO – VAB, IOK, IOG, VGCB, FACOR, Sesa Coke Gujarat & Vazare
CFO - VAB, IOK, IOG, VGCB, FACOR

The CITO based on input from the CISO is expected to be responsible to the senior management, Board, and the Board Committee for reporting risk matter requiring their attention.

5.1.2 Operation and Periodicity of Meeting

The IT steering committee shall meet on periodic (annually) basis or as required for urgent matters. Reports of IT steering committee activities (agendas, decisions) and meetings (including attendance) will be maintained for each meeting.

5.1.3Responsibilities and Authorities

At a minimum, the IT steering committee will deal with and will be responsible for:

- Overseeing the execution of risk management strategies and policies at functional level.
- Ensuring that the risk management initiative for the functions is operationalized as per the risk management framework and polices.
- Reviewing and approving periodically / annually IT Risk Management Report. This report will be provided to the CISO in coordination with members of IT Risk owners.
- Reviewing the annually risk reports from the Operations Managers who are responsible for ensuring risks are managed within their areas of responsibility
- Monitoring risk exposure versus limits as drawn up by the IT steering committee
- Ensuring that the risk register and profiles are reviewed and updated timely and identifying if any risk need to be escalated on annually basis to senior management including board.
- Authority to approve residual risk impacting departments other than IT and CITO to approve residual risks impacting IT Department.

5.2 CISO

The CISO is expected to be responsible to the IT steering committee for IT risk management. Further, he would work with the IT Steering Committee to:

- Oversee the execution of risk management strategies
- Establish and manage the IT Risk Management policy
- Coordinate the risk management program and initiative for the organization as a whole as per the risk management framework and polices and the directives of the IT steering committee.
- Development, maintenance and appropriate distribution of the risk management policy
- Maintenance and coordination of processes for the annual / periodic reassessment of IT risks
- Introduction and ongoing management of the compliance and IT risk monitoring at Sesa Goa

- Report to and update the IT steering committee on the risk management
- Prepare annual Risk Management Report (Annexure V)
- Monitor risk exposure versus limits as drawn up by the IT steering committee
- Ensure that the risk register is reviewed and updated timely
- Ensure that the risk profile is reviewed and updated timely
- Authority to review the framework and policy relating to risk.
- Authority to guide the organization in Risk Assessment and Risk Treatment process.

5.3 Senior Corporate Management

5.3.1 Composition

Senior management shall comprise of following members at the corporate Sesa Goa locations:

- CEO
- CFO
- CITO

5.3.2 Responsibilities

The senior corporate management at corporate function level is expected to be responsible for ensuring that a decision and guidance if required are provided so that risk management process / system is implemented and maintained at the IT level in accordance with:

- Requirements of Risk Management Standard – ISO 31000
- The Sesa Goa Board of Directors' requirements
- The directives of the IT Steering Committee

At a minimum, the committee will be responsible for:

- Annual assessment of risks
- Annually updated IT corporate function Risk Register and Risk Profile (including mitigation plans) if any significant guidance and decision is required.
- Guiding on Monitoring risk exposure versus limits at functional level as drawn up by the IT Steering Committee.

5.3.3 Operation and Periodicity of Meeting

The senior management would be responsible for guidance and decision on risk identification and assessment at the unit / corporate levels. The committee shall review the status of risks in the annually review meeting if required. CISO will coordinate for same.

The CITO and IT function heads will be responsible for identification of risk owners for the risks identified within their business unit / function.

It can be clubbed with the Management meeting and IT ERM can be an additional agenda of the same.

5.4 Risk Owners ('Owners')

IT respective Function Lead are normally identified as risk owners. A proactive approach to risk management involves identifying clear ownership for risk in advance. Ownership supports responsibility, action and accountability. Identification of Risk Owners must be done for each

Risk item. Risk owners are individuals who own, and therefore are deemed accountable for the effective management of one of the specific risk categories. They are essentially the Control Owners.

5.4.1 Responsibilities

They are responsible to the ITSC through their line manager (where applicable) for:

- The operationalization of the framework within their respective areas of responsibility
- Periodic reporting on the status of the relevant risk registers
- Developing risk management and risk mitigation strategies to address risks
- Ensuring compliance with the risk assessment and other requirements as established by the Sesa Goa IT function
- Setting direction and monitor the continual effectiveness of RM processes relating to their assigned risk categories
- Coordinating functional efforts to ensure that management of their specific risk categories is effective
- Ensuring risk response plan has been considered and, where appropriate, developed. Risk response plan includes completing template:
- Identifying action steps to mitigate a risk before it happens
- Establishing action steps to respond to risks which have occurred
- Determining trigger points
- The Risk Owner is not responsible if the risk is outside the control of the organization
- As the control owner he/ she is responsible to ensure that the controls are design, implemented and operating effectively.
- Authority to review and approve the risk treatment plan.

The Risk Owners shall update on a regular basis new risks to be added to the risk register during the year and review the implementation status of mitigation plans. Any risks reassessed as high during the meeting of the Risk Owners shall be escalated to the CISO, as the case may be on an immediate basis.

6. Annexures:

I. List of Risk Categories and Risk Areas

Risk Category	Risk Areas	Suggestive Description
Governance and Strategy	Architecture	This category includes risk related to IT Strategy which need to include the regular monitoring, reviewing and evaluation of existing architecture deployed at Sesa Goa. Architecture planning must involve alignment of hardware, operating systems and software applications with short and long-term business strategy. IT architecture must be upgraded, replaced or modified to keep up the business objectives and IT road map.
Governance and Strategy	Audit	This category includes risks related to audit as per the policy and procedure to ensure regular monitoring for assurance of policy and process compliances.

Governance and Strategy	Human Resource	Risks associated with culture, organisational structure, communication, recruitment, performance management, remuneration, learning & development, retention, succession planning, occupational health & safety and industrial relations, including supporting systems, processes and procedures.
Governance and Strategy	Innovation and Automation	This category includes risk related to rregular proof of concept of new idea/s that need to be undertaken.
Governance and Strategy	Knowledge management	This category includes risk related to Knowledge management session, repository, best practice sharing and cross training FAQ which need to be implemented for learning form past mistakes, events and discussions of Sesa Goa and other organizations.
Governance and Strategy	Policy and Procedure	This category includes risks related to absence or inadequate implementation of information security and privacy related policies and procedures across organization.
Governance and Strategy	Program Management	This category includes risk related to Sesa Goa planning to move towards total outsourcing strategy. Portfolio analysis for outsourcing will need regular reviews. The contract for network, network management and problem management to Airtel, Tata Net and Hitachi are accordingly awarded and need to be reviewed on monthly basis by CITO and IT process owner.
Governance and Strategy	Review	This category includes risks related to periodic review of all the applicable policies, procedures, guidelines, processes, audit reports of Sesa Goa.
Governance and Strategy	Risk Management	This category includes risk related to Risk management process, framework and reports which need to be reviewed by the CITO regularly for adequacy, efficiency and alignment with business objectives.
Governance and Strategy	Strategy	This category includes risk related to IT strategy and road map including aspects of cyber security (including PTS), privacy and data governance which need to be defined in alignment with business strategy and objectives. A short-term and a roadmap must be mapped out for the same, which must be monitored and reviewed for changes in circumstances, laws or business objectives. The outputs must be evaluated for need of upgrade or modification to new technologies to increase the efficiency or decrease cost.

Operations	Access Management	This category includes risks related to unauthorized user access to systems and services.
Operations	Asset Management	This category includes risks associated with the ownership and use of assets including inappropriate protection, handling and maintenance of organization's assets.
Operations	Backup and Restore	This category risks includes risks associated with inadequate backup of information, software and systems. Risk related to Backup retention and protection requirements are also taken in consideration.
Operations	BCP & DR	The planning and processes required to maintain the continuity of business activities or recovery response to a disastrous event which may impact the effectiveness of business operations. The capacity of the DR implementation must be regularly monitored, reviewed and modified as per the existing scenario. In absence of the same the business continuity may be impacted.
Operations	Capacity Management	This category includes risks which are related to the inefficient use of resources resulting from inadequate monitoring, lack of planning and projections made regarding the future capacity requirements. The objective here is to ensure and achieve the required system performance.
Operations	Change Management	This category includes risks which are related to Changes to the organization, business processes, information processing facilities and systems that affect information security.
Operations	Cloud Application and Infrastructure	This category includes risk related to Clear cloud strategy and cloud road map which need to be prepared based on risk-based assessment of cloud adoption, covering aspect of business objective, cloud architecture alignment, data governance, technology vendor landscape, Cyber and privacy security requirement.
Operations	PTS	This category includes risks related to PTS based on risk assessment aligned to NIST 800-82, ISA 62443 and ISO 27001.
Operations	Cryptography	This category includes risks which are related to improper and ineffective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Operations	Data Privacy	This category includes risks which are related to Privacy and protection of personally identifiable information.
Operations	Data Security	This category includes risks which are related to the practice of protecting organization's

		information from unauthorized access, corruption, or theft throughout its entire lifecycle. It also incorporates risk of inadequate implementation of technical safeguards and policies and procedures related to data security.
Operations	Encryption	This category includes risk related to Network and encryption due diligence on network encryption needs to be done by IT and Network Encryption should be implemented.
Operations	Endpoint Security	This category includes risks which are related to securing endpoints, or end-user devices like desktops, laptops, and mobile devices. Endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by malicious actors.
Operations	Environmental Security	This category includes risks related to environment pollution, safety of resources and employees' health. It lists out risks related to damage and interference to the organization's information and information processing facilities due to environmental factors.
Operations	Event Management	This category includes risk related to Proactive and intelligent risk identification which need to be conducted for emerging threats and vulnerabilities as well as recent attacks and events on competitors.
Operations	Incident Management	This category includes risks which are related to ineffective approach to the management of information security incidents, including communication on security events and weaknesses.
Operations	Logging and Monitoring	This category includes risks which are related to inadequate technical controls implemented to record events and generate evidence.
Operations	Mobile Device and Teleworking	This category includes risks which are related to the security of teleworking and use of mobile devices.
Operations	Network Security	This category includes risks which are related to the protection of information in networks and its supporting information processing facilities.
Operations	Operation management	This category includes risk related to Sesa Goa's migration to a Tier-4 architecture data centre to improve operation resiliency and prevent performance degradation.

Operations	Operations Security	This category includes risks which are related to the correct and secure operations of information processing facilities.
Operations	Physical Security	This category includes risks which are related to unauthorized physical access, damage and interference to the organization's information and information processing facilities.
Operations	Project Management	This category includes risk related to Project management framework and process which need to be designed and implemented to align with Sesa Goa plans and objectives. IT project more than xxx crores must have project sponsor, steering committee and Project manager. Project will be regularly reviewed as per project plan.
Operations	Removable Media	This category includes risks which are related to the unauthorized disclosure, modification, removal or destruction of information stored on media.
Operations	Review and Audit	This category includes risks which are related to inappropriate review and audit mechanism to ensure that information security and operated in accordance with the organizational policies and procedures.
Operations	SDLC	This category includes risks which are related to the security of information and information systems across its entire lifecycle. This incorporates risks and vulnerabilities from the start of the project till the final acceptance of the software product.
Operations	Unified Communications	This category includes risks which are related to disclosure of information through unrestricted access to public portals, data sharing sites, video conferencing software, improper e-mail communications and other allied risk related to virtual communication.
Operations	Vendor risk management	This category includes risk related to Alternate vendors for critical services which need to be identified and selected. Due diligence for security and privacy and POC need to be performed. Contracts with vendors which need to include clauses relating to information security, privacy and continuity incidents the vendor contracts need to be monitored regularly for changing services, laws and regulations.
Financial	Financial	This category includes risk related to Budget allocation needs to be done with regards to policy, procedure, roles and responsibilities. KPI of budget item/s must be mapped to process owner and reviewed and monitored regularly.

Legal and compliance	Compliance	This category includes risk related to Monitoring and review of applicable laws and regulation and vendor contracts which need to be done regularly through attending various conferences, subscribing to Journal and getting alerts from external as well as legal team to ensure compliance.
Legal and Compliance	Contract (Vendor and Third-Party) Monitoring and Management.	This category includes risk related to SLAs and NDAs signed with every vendor and third-party. The SLAs and NDAs must be monitored and managed for changes in service conditions and legal and regulatory compliance.
Legal and Compliance	Regulatory Compliance	This category includes risk related to IT and Data Governance Regulations which are applicable to Sesa Goa. The requirements of applicable regulations need to be identified and monitored for changes.
Legal and Compliance	Review	This category includes risks related to compliance to applicable standards and regulations. The audit dept needs to make proper documentation and conduct timely review of exceptions and deviations.
Legal and Compliance	Software Compliance	This category includes risks which are related to the usage of non-licensed software or open-source software, lack of tool for software utilization, review, monitoring and compliance of authorized software installed and usage of old software versions.

This list may be modified in future to add / modify new risk baskets that may emerge.

2. Annexure 2 - Risk Assessment for PTS systems

The methodology for Risk Assessment for PTS 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.

Risk Scorecard Template

Risk Scorecard Template.docx

I. Risk Register Template

Risk Register Template.xlsx

II. Risk Profile Template and Risk Treatment Plan

Risk Profile and Risk Treatment Template.d

III. Risk Measurement Matrix for IT

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

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. crore of business loss	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 the viability of the organization.	Critical application / service failure affecting multiple Operations resulting in serious operational impact or impacting more than .75 lakh -1 crore	Regulatory or contractual breach resulting in moderate penalties leading to formal enforcement action by the authority or Significant breaches, significant financial penalties & prosecution of staff / stoppage of business. Multiple litigations	Prolonged negative focus and concerns from the stakeholders resulting in serious reputational impact to the organization.
Major (3)	Any single or cumulative potential loss could range between 5%-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 .50 lakh-75 lakh	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 .50 lakh to .025 lakh 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 .025 lakhs	No legal or regulatory impact to the organization	No reputational impact to the organization

Rating	B) Likelihood Criteria
	Occurrence and Probability

Very High	**5**	Likely to occur once in 3-6 months or known incident is last 3-6 months
High	**4**	Likely to occur within 1 year or known incident in last 1 year
Moderate	**3**	Likely to occur within 1-3 years or known incident in last 1-3 years
Low	**2**	Likely to occur within 3-5 years or known incident in last 3-5 years
None/Negligible	**1**	Likely to occur within 10 years or known incident in last 10 years or has happened in past
Note: Precise quantification of the Rupee value impact of many risks is often impractical, since the ultimate cost would depend on a significant number of variables. Where values can be assigned it is necessary to look at the above effects over a future time period rather than that particular financial year. For categories as given in Annexure I where quantification is not possible, the likelihood and impact score may be given on the above scale and criticality of risk determined based on the combined scores		
*** To be specified by the IT Steering Committee** **** IT Steering Committee may enhance or reduce the financial limits**		

Risk Definitions

Terms	Definition
Risk	Effect of uncertainty on objectives.
Risk Management	Coordinated activities to direct and control an organization with regard to risk.
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Risk Source	Element which alone or in combination has the potential to give rise to risk.

Event	Occurrence or change of a particular set of circumstances.
Consequence/ Impact	Outcome of an event affecting objectives.
Likelihood	Chance of something happening.
Control	Measure that maintains and/or modifies risk.
Risk in Risk Register	It is the combination or Risk Source and Risk Event.