ITI LIMITED
(A Government of India Undertaking)

ITI ENTERPRISE RISK MANAGEMENT MANUAL

ITI Limited
ITI Bhavan
Bangalore-560016

Amendment record sheet

Amendment No. / Date	Section Changed	Details of Amendments	Signature
V1.0 / 12-Feb-2021	Entire Document	Initial Version	

This Policy has been approved by the Board of Directors of ITI Limited at its meeting held on 22nd June, 2021. Any amendment to the policy must be done with the approval of the Board. This Policy will be reviewed every two years or earlier if required by any circumstances.

Disciplinary action shall be initiated for any violation of this policy or the guidelines framed hereunder.

Table of Contents

Chapter 1: Introduction

Achievement of business and financial objectives sustainably is of paramount importance for an Organization. The Top Management of any organization is always under pressure to perform and to achieve the business targets. When periodical reviews are undertaken, related questions surface. Some such questions could be "What sort of roadblocks/opportunities may be encountered while achieving the business goals? What are the risk factors faced by the organization? To what extent can these risk-factors impact the achievement of the business objectives? How can these risk factors be treated? How to regularly control and monitor the risk-factors?" etc.

Enterprise Risk Management (ERM) provides an answer to such questions. ERM is defined as a continuous and structured process of identifying all external and internal risk-factors; assessing their impact on the achievement of the organization's business and financial targets; prioritizing the risk-factors; exploring alternatives for treating the risks; and controlling and monitoring such risks.

Thus, ERM encompasses the entire gamut of the organization's operations and is not limited to a single event or circumstance impacting the organization's functioning. It is a dynamic process involving people at all levels, covers every aspect of the organization's resources and operations and takes a holistic view of the entire organization for the purpose of risk management.

This document is intended to provide guidance on implementing an effective Enterprise Risk Management (ERM) program in ITI Ltd (hereinafter also referred to as the Company or as the Organization). This ERM framework has been developed based on the following guiding principles:

- The ERM framework should demonstrate adherence to ISO 31000, ISO/IEC 31010 and other applicable standards;
- The ERM framework should provide a forum for risks to be appropriately considered, discussed, debated, and factored into strategic business decisions;
- Decisions should be made with appropriate consideration of the impact on the overall Organization, not just the individual lines of business;
- The ERM Governance should focus on and enable making risk management processes proactive rather than reactive;
- The risk governance structure should consider and reflect the roles and interaction with related functions, including compliance, internal audit, etc.;
- The ERM must cover following areas:
    - Business units that take risk and manage the risks they take;
    - ERM Governance organization that provides policy, guidance, recommendations, risk reporting and analysis; and,
    - Independent assurance functions such as internal audit, compliance, vigilance, etc.
- The ERM framework model should continually improve over time

This document lays down the framework for Enterprise Risk Management at ITI Limited and defines the policy for the same. The objective of ITI's ERM framework is to manage and in the long term, achieve a substantial reduction in risk exposure and maintain it at an acceptable level. The aim is to maintain the balance between compliance and performance. It seeks to identify risks inherent in the business operations of the Company and provides guidelines to define, measure, report, control and treat the identified risks. In ITI, risk management includes both negative meaning like threat and positive meaning like opportunity.

The objective of the ERM framework manual is to ensure that the Company has proper and continuous risk identification and management processes. Risk management process will be an integral part of management and decision-making and is integrated into the structure, operations and processes of ITI. Integrating risk management into the Organization is an iterative and dynamic process. Therefore, risk management will be a part of, and not isolated from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

Chapter 2: Purpose

The main purpose of the Enterprise Risk Management Framework is to provide appropriate guidance to the Management towards the Business and Operational Risks across ITI. It is the responsibility of the ITI Board, Management, Employees, Internal and External Stakeholders at all levels to ensure that risks are fully understood, appropriately identified and adequately managed in accordance with the policy. The main approach has been based on the Standard specified in ISO 31000:2018, *Risk management – Guidelines*, which provides principles, framework and a process for managing risk as depicted in the figure in the following sections. Using ISO 31000 guidelines will help increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. Adherence to a globally recognized Risk Management framework such as ISO 31000 guidelines would also help enhance the confidence of the stakeholders in the Organization's risk management policies and procedures.

Chapter 3: Scope

This Enterprise Risk Management Framework shall be applicable to all ITI employees, all units, offices, and its internal and external stakeholders. It provides a mechanism of reporting system by the Units / offices. This scope has been defined based on the Context Analysis of the Organization.

Chapter 4: Compliance

The compliance with the ERM framework is mandatory. Any deviation or exceptions shall require prior approval of ITI's Board of Directors.

The Risk Management Framework of ITI Limited is framed to cover the following regulatory requirements:

- Companies Act, 2013
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015
- DPE Guidelines

Chapter 5: ERM Policy

ITI has established the ERM policy based on the guiding principles and its strategic business plan. The ERM policy statement is as given below:

"ITI Limited is committed to the effective management of risk, which is central to the continued growth and profitability of the company. The risk management policy of the company will provide a framework to:

- ***set objectives and establish principles for action for risk management based on business objectives, legal or regulatory requirements, and contractual obligations;***
- ***align risk management with the organization's strategic context for effective decision making;***
- ***embed risk management within the organization by communicating with and involving all employees in the identification of risks to mitigation.***
- ***establish criteria (key risk indicators) against which risk will be evaluated, measured and reported.***
- ***ensure resources are available to assist those accountable and responsible for managing risk.***
- ***conduct and implement risk management activities in an agreed, controlled manner so that divergent objectives are harmonized***
- ***achieve a risk management capability that meets changing business needs and is appropriate to the scale, complexity and nature of the organization.***
- ***monitor material changes to the company's risk profile and disclose in accordance with the company's Continuous Disclosure Policy."***

This Framework also specifies the ongoing management and maintenance of the risk management capability, including:

- assigning of accountabilities and responsibilities at appropriate levels within the Organization
- updating and communicating of the risk mitigation plans, particularly when there are significant changes in personnel, processes, markets and technology.
- reviewing the effectiveness of the risk management framework and making improvements to it, particularly when there are significant changes in personnel, processes, markets or technology.
- ensuring that the framework for managing risk continues to remain appropriate to the changing landscape.

The defined risk policy and objectives will be applicable at the enterprise level and effectiveness of risk management will be determined based on performance results.

Detailed objectives that are expected to be achieved through the implementation of this Risk Management Framework are:

- Establish an ERM Framework that will define interrelationship and linkage between the various components of Risk Management.
- A Companywide approach by integrating risk management processes with: Business Strategy; Project Management; Process and Decision Making; Audit and General Governance Functions.
- Establish a consistent, replicable, flexible, systematic and Organization wide process to Identify, assess, rank, escalate, treat, monitor and report risks inherent in the Organization.
- Selecting the appropriate risk management approach and transferring or avoiding those risks that the business is not willing or competent to manage;
- Establish a Risk Management Organisation and Governance structure with clearly defined roles and responsibilities and updating these on a continual basis.
- Maintain the necessary documentation (Risk Register, Risk Assessment Templates, Risk Profile, Loss Database and Risk Escalation Matrix) for each stage of the risk management process.
- Perform risk reporting to the Board.
- Perform periodic reviews of all risks recorded in the risk register and risk profiles to ensure that the current assessment remains valid.
- Promote consistency and transparency in methodology, assessment and management processes.
- Promote risk aware culture throughout ITI Limited by organizing periodic training and awareness campaigns.
- Protect the interests of the shareholders.
- Recognize that timely and accurate monitoring, review, communication and reporting of risk is critical to:
    - providing early warning mechanisms for the effective management of risk occurrences and consequences.
    - providing reasonable assurance to management, the Board and shareholders;

Chapter 6: ERM Framework

ERM involves listing the objectives of the Organization; identifying the risk-factors that could adversely impact the achievement of each of the objectives; assessing the impact of the risk-factors on the achievement of each of the objectives; finding alternatives for mitigating the risk-factors and taking steps to control and monitor the risk-factors on a regular basis. All these steps are modelled in the ERM framework described below.

This ERM framework is designed to fully integrate the risk management process into the Organization's business processes. The framework assures that an Organization-wide process is supported iteratively and effectively. It means that risk management will be an active component in governance, strategy and planning, management reporting processes, policies, values and culture.

Major elements of ITI's ERM model "**CEIM**" include the following:

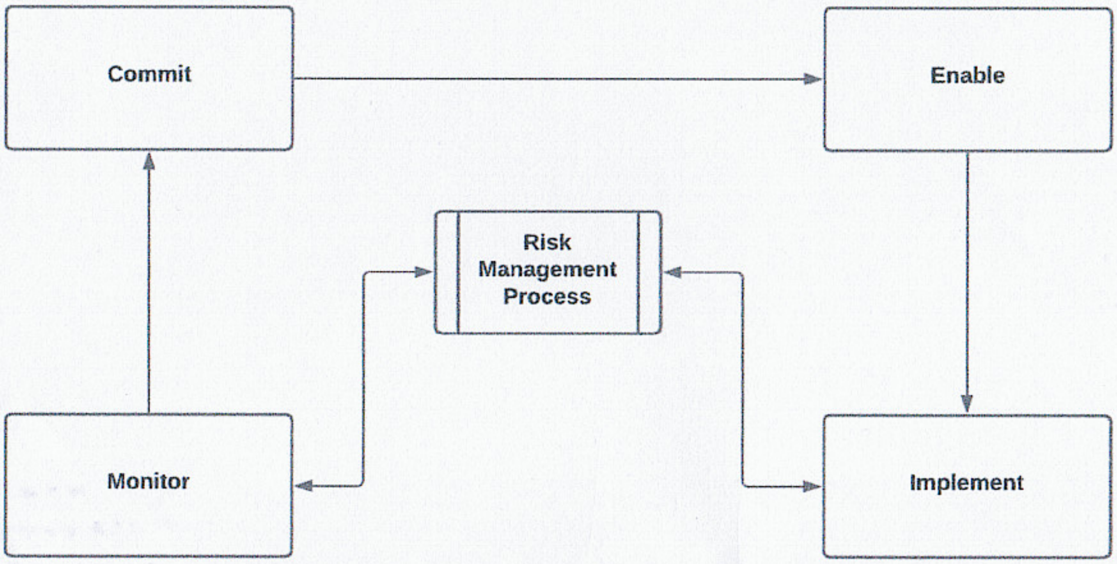
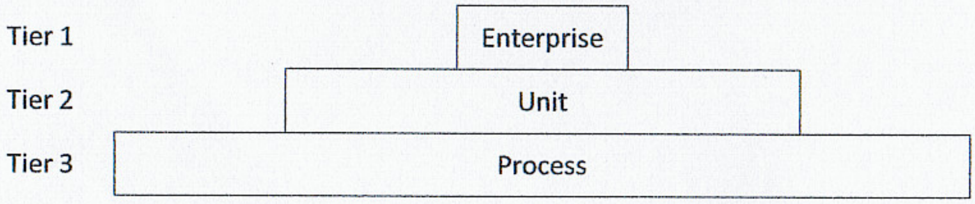


Figure 1 - ERM Model

- **Commit:** Demonstrate commitment of the Organization towards implementing ERM. This stage includes establishing the following.
  - Policy Statement
  - Standards
  - Process
  - Resources

  - Roles & Responsibilities
- **Enable:** Communicating and training all relevant stakeholders for effective implementation of ERM. This stage includes establishing the following.
  - Communication plan
  - Training Plan
- **Implement:** Practice as per established ERM framework expectations. This stage includes establishing the following
  - Stakeholder Analysis
  - Governance Set up (Committees, Groups)
  - RM Champions / Risk Owners
  - Risk Management
  - Risk Database (to collect experiences and lessons learnt)
  - Document Management
- **Monitor:** Review, monitor ERM implementation and take necessary corrective and preventive actions. This stage includes establishing the following.
  - Risk Monitoring
  - Governance reporting
  - Improvement Plan

The Risk Management Process must address all areas and levels of the Organization. Following diagram shows the three tiers of the Organization where risk management would be performed and how the ERM framework integrates it into a holistic approach:



As depicted above, the basic or ground level risk management is performed in Tier 3 at the Process level (such as within a project, departments such as production, material management, HR, information technology, etc). Here, risks are identified at the Process level considering the operational aspects. To record and manage the risks, each Process will use the risk register format that is appropriate for it. The significant risks in this tier will get escalated to the Unit level (Tier 2) for further management.

Apart from risks escalated from Tier 3, risks can also be identified independently and managed at Tier 2. To record and manage the risks at Tier 2, a unit-level risk register in the risk register format as defined in Annexure 5: Template for Enterprise Risk and Opportunity Register needs to be used. The significant risks in Tier 2 will get escalated to the Enterprise level (Tier 1) for further risk management.

Apart from risks escalated from Tier 2, risks can also be identified independently and managed at Tier 1. To record and manage the risks at Tier 1, an enterprise-level risk register in the risk register format as defined in Annexure 5: Template for Enterprise Risk and Opportunity Register needs to be used.

The ERM framework has also defined the broad categories of risks. These risk categories are further divided into risk sub-categories. A detailed description of these risk categories and sub-categories is provided in the risk register format provided in Annexure 5: Template for Enterprise Risk and Opportunity Register.

The risk management process is further detailed in Chapter 7: below.

Chapter 7: Risk Management Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

A high-level Risk Management Process includes various steps as shown in the following diagram.

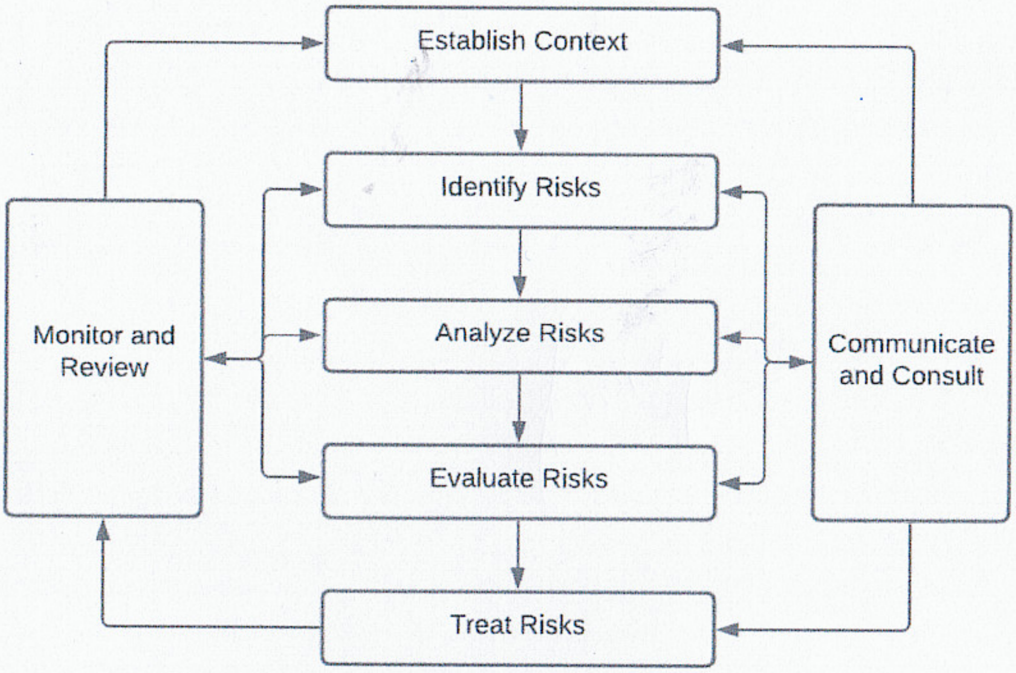


Figure 2 - Enterprise Risk Management Process

7.1 Establish the Context of the Organization:

The context of the risk management process is established from the understanding of the external and internal environment in which the Organization operates and should reflect the specific environment of the activity to which the risk management process is to be applied.

The Organization establishes the external and internal context of the risk management process by considering the factors mentioned in clause 5.4.1 in the ISO 31000 standard.

This step is done as context analysis, a template for which is provided in Annexure 4: Template for ERM Context Analysis.

7.2 Defining the Risk Criteria

The Organization determines the amount and type of risk that it wishes to take, relative to its objectives. Criteria to evaluate the significance of risk and to support decision-making processes are established which is available in the risk register in the form of risk score matrix. Risk criteria is aligned with the risk management framework and customized to the specific purpose and scope of the activity under consideration. Risk criteria also reflects the Organization's values, objectives and resources and is consistent with policies and statements about riskmanagement. The criteria is defined taking into consideration the Organization's obligations and the views of stakeholders.

While risk criteria is established at the beginning of the risk assessment process, they are dynamic and are continually reviewed and amended, if necessary.

To set risk criteria, the following are considered:

- the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);
- how consequences (both positive and negative) and likelihood will be defined and measured;
- time-related factors;
- consistency in the use of measurements;
- how the magnitude of the risk is to be determined;
- how combinations and sequences of multiple risks will be taken into account;
- the Organization's capacity

7.3 Risk Identification

Once the objectives and assumptions of the Organization have been established, the potential risks that may have an effect on the achievement of these objectives are identified. Thisinvolves continuous identification of events that may have impact on the Company's ability to achieve goals. Processes have been identified by the Company and their key activities have been selected for the purpose of risk assessment. Identification of risks, risk events and their relationship are defined on the basis of discussion with the risk owners and secondary analysis of related data, previous internal audit reports, information from competition, market data, Government Policies, past occurrences of such events etc. Significant issues under Risk identification are to be tagged with appropriate risk categories.

7.4 Risk Analysis

Risk analysis considers factors such as:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of existing controls;
- sensitivity and confidence levels.

The likelihood of the occurrence of a risk is determined based on the Likelihood Ratings table defined in the ERM Risk Register which is available in Annexure 5: Template for Enterprise Risk and Opportunity Register.

Similarly, the impact of the occurrence of a risk on the achievement of the Organization's objectives is determined based on the Impact Ratings table defined in the ERM Risk Register which is available in Annexure 5: Template for Enterprise Risk and Opportunity Register.

7.5 Risk Evaluation

Based on careful risk analysis, risk score for the risk is computed by multiplying its likelihood rating with its impact rating. The Risk Prioritization Matrix, defined in the ERM Risk Register available in Annexure 5: Template for Enterprise Risk and Opportunity Register, is then used to translate the risk score into the priority that must be accorded to managing the risk.

This risk evaluation is done to support decision making. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.

The outcome of risk evaluation is recorded, communicated and then validated at appropriate levels of the Organization.

7.6 Risk Treatment

Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options;
- planning and implementing risk treatment;
- assessing the effectiveness of that treatment;
- deciding whether the remaining risk is acceptable;
- if not acceptable, performing further treatment

Risk treatment will address likelihood or impact or both.

Brainstorming is done to identify the various ways of treating the risk and based on mutual consent one treatment option is chosen. A detailed treatment plan will be prepared and implemented.

Following guidelines are used for risk treatment:

1. **Risk Score 9**: Mandatory risk treatment and monitoring and review by top management including effectiveness check. If no feasible treatment options available, monitoring and review must be performed by top management
2. **Risk Score 6**: Risk treatment is optional. Mandatory monitoring and review of top management
3. **Risk score less than 6**: Risk treatment and monitoring & review by top management is optional

If risk treatment introduces new risk, it must be taken up as a separate risk and managed according to the process. Once the Risk treatment is complete and effectiveness is achieved, residual risk must be computed and a re-evaluation is performed to determine if the new risk score needs further treatment and actions to be taken accordingly. If a new risk score doesn't meet risk criteria for treatment, monitoring of risk by top management is done.

The treatment plan should include:

- the rationale for selection of the treatment options, including the expected benefits to be gained;
- those who are accountable and responsible for approving and implementing the plan;
- the proposed actions;
- the resources required
- the performance measures;
- the constraints;
- the required reporting and monitoring;
- when actions are expected to be undertaken and completed
- effectiveness check

Risk treatment options are also categorized based on whether it is a risk (threat) or an opportunity.

Treatment Options for Risk:

- Avoid: Avoid the process or the activity that has potential risk
- Accept: Accept the risk and do nothing further
- Mitigate: Take actions to reduce likelihood or impact or both
- Transfer: Transfer the risk to other entity

Treatment Options for Opportunity:

- Exploit: Accept the opportunity and exploit it
- Decline: Decline the opportunity and do nothing further
- Enhance: Take actions to increase the likelihood or impact or both
- Share: Share the opportunity with others

7.7 Communicate and Consult

The purpose of communication and consultation is to assist relevant stakeholders in understanding 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, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate 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.

Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

Communication and consultation aim to:

- bring different areas of expertise together for each step of the risk management process;
- ensure that different views are appropriately considered while defining risk criteria and evaluating risks;
- provide sufficient information to facilitate risk oversight and decision-making;
- build a sense of inclusiveness and ownership among those affected by the risk

7.8 Recording and Reporting

The risk management process and its outcomes are documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the Organization;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Reporting is an integral part of the Organization's governance. Following are the list of documents that are primarily used for reporting purposes:

- Context Analysis Document
- Risk Register
- Risk Treatment Plan with status
- Executive Summary of Risk Status to the top management

All the above documents are placed in soft versions and in a central repository with appropriate access rights so that all authorized personnel will have access to them.

The reporting activities need to be conducted as per the below Communication Matrix:

S. No.	Review	Frequency	Responsibility	Participants	Input	Outcome
1	ERM Review by Board of Directors	Half-Yearly	Board of Directors	Board of Directors, ERMGC, ERMSC, ERO	ERM Status Report by ERO	Advise by the Board
2	ERM Review by ERMGC	Quarterly	ERMGC	ERMGC, ERMSC, ERO	ERM Status Report by ERO	Advise by the ERMGC
3	ERM Review by ERMSC	Monthly	ERMSC	ERMSC, ERO	ERM Status Report by ERO	Directions by the ERMSC
4	ERM Review by URMC	Monthly (prior to review by ERMSC)	URMC	URMC, URO	ERM Status Report by URO	Directions by the URMC
5	Risk Management Review at Process level	Ongoing Activity	Process Owner	Process Owner, Process Team	Risks and Opportunities identified by the Process Team	Risk Reporting to URO

7.9 Monitor and Review

A regular monitoring mechanism is established to ensure that the decision taken is implemented.

Monitoring of Risk Management processes and its outcome is done in order to continually improve it. Any improvement ideas for ERM framework and processes are incorporated as per continual improvement process.

Risks are reviewed and monitored periodically, based on the criteria mentioned in the risk treatment section so that unpleasant surprises and barriers are reduced and golden opportunities are discovered.

7.10 Risk Management Organization Structure

The Governance structure of Risk Management in ITI will be as depicted below:

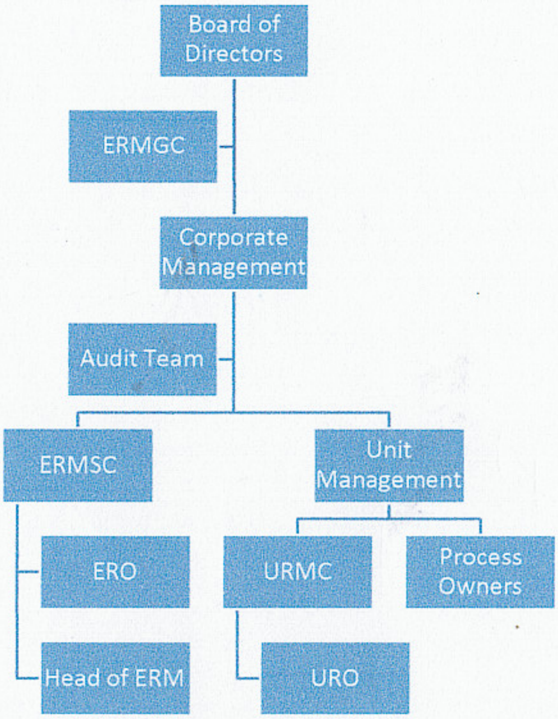


Figure 3 - Risk Management Organization Structure

The various risk management committees within ITI are as follows:

1. Enterprise Risk Management Governance Committee (ERMGC) is at the Board Level
2. Enterprise Risk Management Steering Committee (ERMSC) is at the Corporate Level
3. Unit Risk Management Committee (URMC at each Unit level)

The constitution of the above Committees will be as follows

1. Enterprise Risk Management Governance Committee ('ERMGC')

Director – HR (Chairman of ERMGC)
Director - Finance
Independent Director (One)
Head of PP
Head of Operations - Enterprise Risk Officer (ERO) – Convener

2. **Enterprise Risk Management Steering Committee ('ERMSC')**

Director – Production (Chairman of ERMSC)
Head of Operations – Enterprise Risk Officer (ERO)
Head of PP
Head of Corporate Finance
Head of Corporate Marketing
Head of Corporate HR
Head of ERM (Convener)

3. **Unit Risk Management Committee ('URMC')**

Unit Head/Office Head – Chairman
Head of Production
Head of R&D
Head of Finance
Head of MM
Head of Planning
Head of HR
Unit Risk Officer ('URO') – Convener

Notes on Risk Management Committees:

1. CMD is an invited member to the ERMGC
2. Chairman of each of the committees may co-opt any person to join the committee for Professional advice whenever required.
3. Head of ERM reports administratively to Director – HR and functionally to ERMSC.
4. Functional Points of Contact (POC) at the Corporate Office are as follows:

- RO – Finance
- RO - MM
- RO - PP
- RO - HR
- RO – Operations

The responsibilities of the above ROs for their respective corporate departments will be same as that of the Unit Risk Officer (UROs) as outlined in the section Roles and Responsibilities.

5. Any changes to the organizational structure will require approval from the Management Committee (MC).

7.11 Roles and Responsibilities

The Roles and Responsibilities for various levels of ITI in the ERM policy are as given below:

S. No.	Role	Responsibility
1	Board of Directors	▪ Oversee the establishment of an Enterprise Risk Management (ERM) system in the context of the relevant legislation, broader Governance framework and ITI Bye-Laws. ▪ Oversee and provide guidance in the formulation, adoption and implementation of the ERM Policy. ▪ Monitoring / Review of the ERM outcomes on an ongoing basis. ▪ Guidance and support to ERMGC and the Management on effective risk management. ▪ The Board shall have the sole discretion to deal with certain risks (called as Key or Highly Sensitive Risks) in the manner it deems fit. Treatment of such risks, effectiveness of their treatment plans and review of the strategy will be directly discussed by the Board members with the ERMGC.
2	Enterprise Risk Management Governance Committee (ERMGC)	▪ Oversee the establishment of Enterprise Risk Management system within the broader Governance guidelines, ▪ Provide guidance in formulation of ERM policy, consider and approve design of ERM Function, ▪ Set standards for ERM Documentation ▪ Ensure that the Organization's processes and internal controls reflect new and changing risks and operational deficiencies. ▪ Evaluate ERM Framework and assess its effectiveness, monitor emerging issues ▪ Update the Board on the effectiveness of ERM Framework, ▪ Advise ITI Management on ongoing basis regarding risks and treatment Plans
3	Enterprise Risk Management Steering Committee (ERMSC)	▪ Review and approve the ERM framework and submit it for approval of the ITI Board. ▪ Spearhead ERM initiative within the Organization. ▪ Monitor emerging issues. ▪ Oversee plans to define and implement Risk Treatment strategies ▪ Improve Risk Management techniques and enhance awareness. ▪ Set Standards for Risk Documentation and Monitoring. ▪ Recommend training program for employees/Officers with specific ERM responsibilities. ▪ Facilitate sharing of ERM related best practices across the Organization

S. No.	Role	Responsibility
		▪ Review, approve and submit the ERM report for review by the ITI Board.
4	Enterprise Risk Officer (ERO)	▪ Lead the ERM function across the Organization as per the ERM Policy and the directives of ERMGC and ERMSC. ▪ Review the Development, Maintenance and appropriate distribution of the ERM Policy and standards. ▪ Review and submit the ERM report to ERMGC. ▪ Convene the ERMGC meetings
5	Head of ERM	▪ Support ERO in effectively ensuring the implementation and compliance to the ERM Framework across the Company ▪ Coordinate with the Units and with the various Risk Management Committees ▪ Act as custodian of the ERM documents at Corporate level ▪ Coordinate the ERM activities across the Organization as per the ERM Policy and the directives of ERMGC and ERMSC. ▪ Development, Maintenance and appropriate distribution of the ERM Policy and standards. ▪ Prepare ERM report and submit the same to ERMSC. ▪ Convene the ERMSC meetings ▪ Act as backup for ERO during absence of ERO
6	Unit Risk Management Committee (URMC)	▪ Oversee the ERM strategies and plans at the unit. ▪ Ensure that the ERM initiative in unit is as per the ERM policy and directives of ERMSC. ▪ Review and approve Unit level ERM report and send the same to Unit head and ERO.
7	Unit Risk Officer (URO)	▪ Lead and Coordinate the ERM function across the unit as per the ERM Policy and the directives of ERMGC, ERMSC and URMC. ▪ Assist URMC in execution of ERM strategies and policies in the Unit. ▪ Assist URMC in the coordination of the ERM initiative for the Unit as per ERM Policy and the directives of ERMSC. ▪ Receive and Review ERM updates from the Risk Owners. ▪ Compile and prepare unit-level ERM Report and submit to URMC for review. ▪ Assist and ensure that the Unit level Risk Register and Risk Treatment Plans are reviewed and updated on time ▪ Act as custodian of the ERM documents at Unit level
8	Process Owners	▪ Ensure operationalization of the ERM framework within their respective area of responsibility.

S. No.	Role	Responsibility
		▪ Periodic reporting on the status of relevant risks ▪ Ensure compliance with the risk assessment as established by ERMSC ▪ Set Direction and monitor the continual effectiveness of ERM processes relating to their respective processes ▪ Coordinate Functional efforts to ensure that the risk management of their processes is effective ▪ Ensure Risk Treatment Plan has been considered and developed. Risk Treatment Plan includes completing the following details - Identifying action steps to mitigate a risk before it occurs - Establishing action steps to respond to risks if they occur - Determining Trigger Points

7.12 Audit

Audit must be conducted annually in order to ensure the compliance to, effectiveness of and improvements in the ERM framework. Its objective will include:

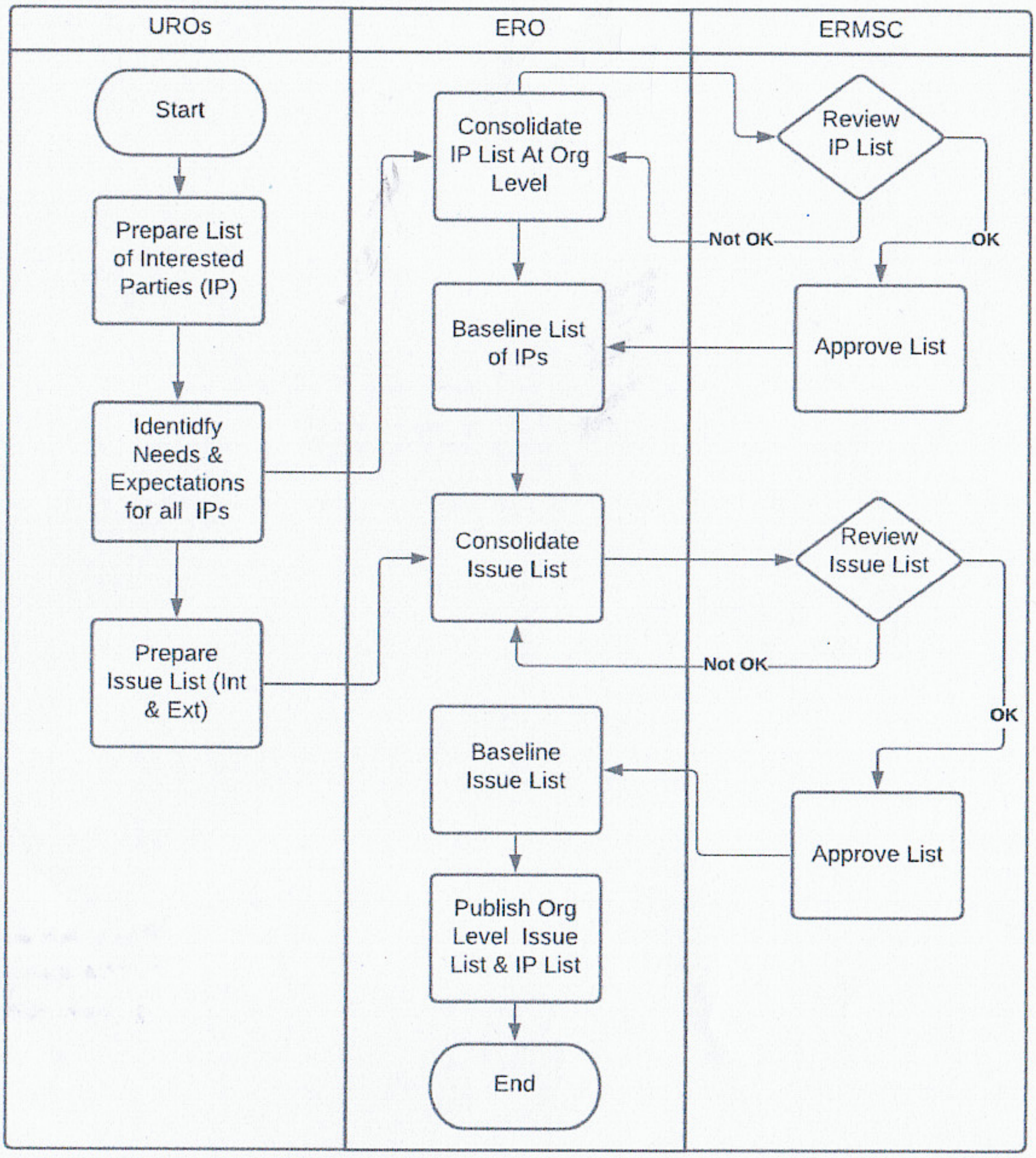
- Provide effective, independent and objective evaluation of status of Enterprise Risk Management across ITI.
- Assess the efficiency and effectiveness of Risk Profile and Performance against established treatment plans.

While Audit team is administratively under the Corporate Management, it will functionally report to the ERMGC and will communicate Audit findings directly to the ERMGC.

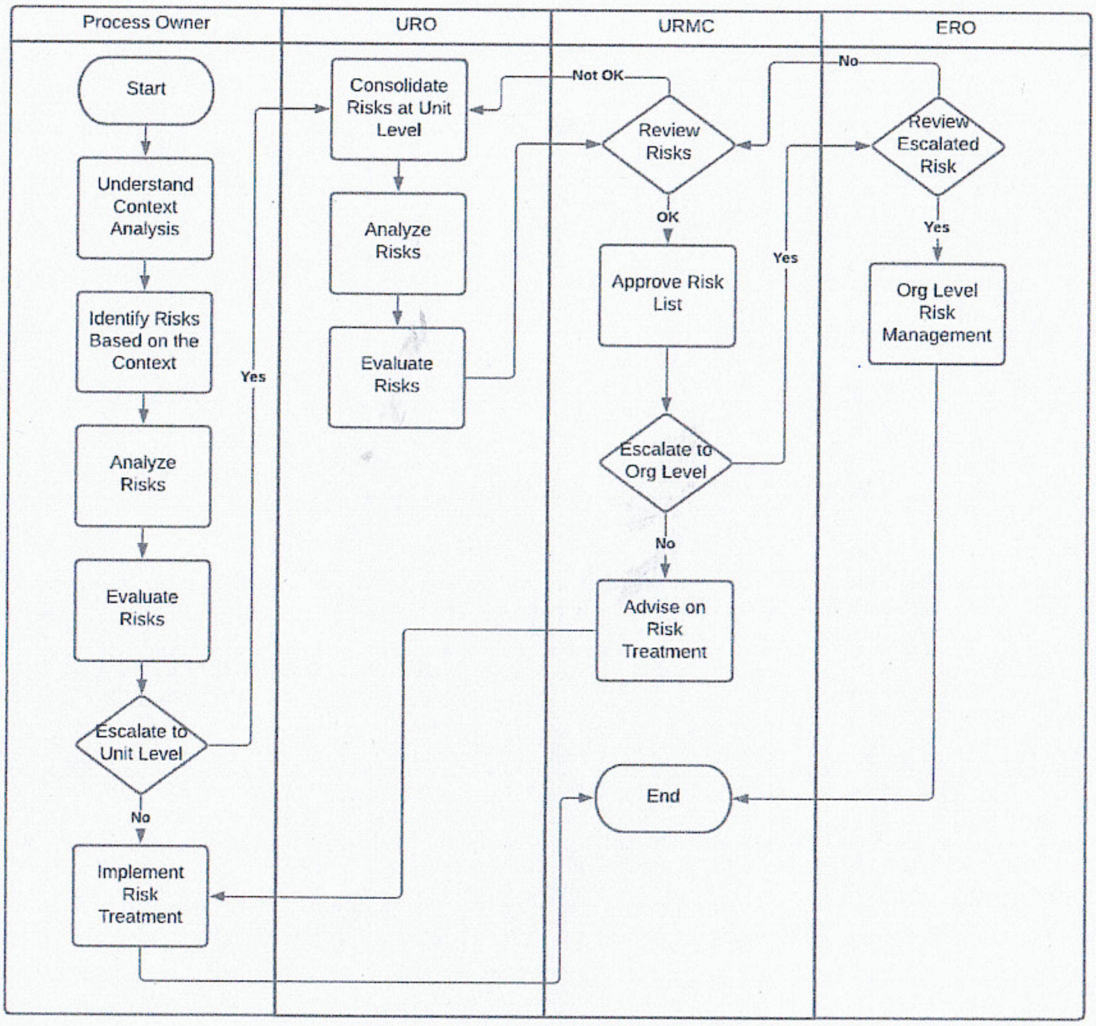
Chapter 8: Disclosures

The Board's annual report shall contain a statement indicating the Development and Implementation of an Enterprise Risk Management (ERM) Policy for the Company as per the DPE Guidelines on Corporate Governance.

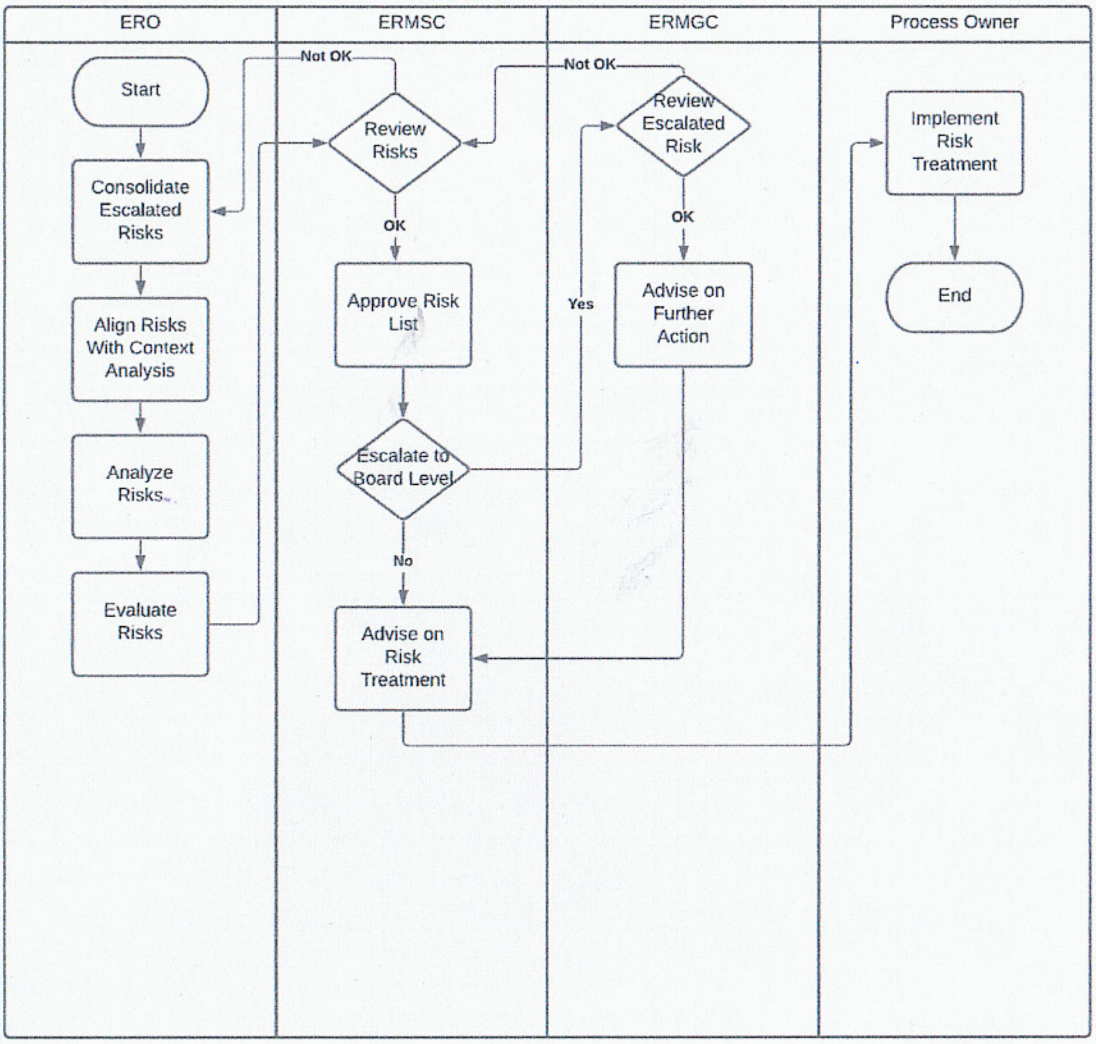
Annexure 1: Flow Chart of Context Analysis - Organization Level


UROs
ERO
ERMSC
Start
Prepare List of Interested Parties (IP)
Identidfy Needs & Expectations for all IPs
Prepare Issue List (Int & Ext)
Consolidate IP List At Org Level
Baseline List of IPs
Consolidate Issue List
Baseline Issue List
Publish Org Level Issue List & IP List
End
Review IP List
Not OK
OK
Approve List
Review Issue List
Not OK
OK
Approve List

Annexure 2: Flow Chart of Risk Management Process - Unit Level



Annexure 3: Flow Chart of Risk Management Process - Corporate Level



Annexure 4: Template for ERM Context Analysis

The embedded file has the template to be used for performing the ERM Context Analysis. It also provides detailed instructions for using it.

Template - ERM
Context Analysis - V1.

Annexure 5: Template for Enterprise Risk and Opportunity Register

The embedded file has the risk and opportunity register template. It also provides detailed instructions for using it.

Template - Enterprise
Risk and Opportunity

Annexure 6: Template for Risk Treatment Plan

The embedded file has the template for documenting the Risk Treatment Plan for a particular risk.

Template - Risk
Treatment Plan - V1.0

Annexure 7: Glossary of Terms and Definitions

Unless otherwise noted, ITI applies the definitions of key terms according to ISO 31000.

ITI's specific definitions and abbreviations are as given in the table below.

S. No.	Term	Description
1	CMD	Chairman and Managing Director
2	ERM	Enterprise Risk Management
3	ERMGC	Enterprise Risk Management Governance Committee
4	ERMSC	Enterprise Risk Management Steering Committee
5	ERO	Enterprise Risk Officer
6	MM	Material Management
7	PP	Projects and Planning
8	RO	Risk Officer
9	URMC	Unit Risk Management Committee
10	URO	Unit Risk Officer

Annexure 8: References

This ERM Framework is based on the following standards / guidelines:

1. ISO 31000:2018 Risk Management – Guidelines
2. IEC 31010:2019 Risk Management – Risk Assessment Techniques

This ERM Policy is supported by, and linked to, specific ITI policies and standards as issued from time to time. These Policies and Standards include, but are not limited to:

- Personal Manual
- Corporate Code of Conduct
- Accounting Policies
- Anti-Sexual Harassment – Safe Work Environment Policy
- Whistle Blower Policy
- Company Social Responsibility as per Government Guidelines
- Material Management Manual

ERM Context Analysis

Change History

Document Change History

Version	Date	Completed By	Reason for Change

Context Analysis Log: Interested Parties List

S. No.	Interested Party	Internal / External	Reason for Inclusion	Needs and Expectations
1	Customer	External	Recipient of organization's products and services	Quality service in-time, customer satisfaction & quick complaints resolution, credible & reliable outputs
2	Staff / Workers	Internal	Direct / indirect contribution towards product and service realization	Job security, communication & compliance to safety norms, growth, Skill development/enhancement, Recognition, Rewards & good working atmosphere.
3	Public	External	Affected by organization's activities	Compliance to law, environmental protection, safety
4	Vendors	External	Supplier of goods and services - direct / indirect contribution towards product and service realization	Continuity of business, proper communication of requirements and feedback, timely payment
5	Investors	Internal	Affected by organization's performance and financial health	Return on investment & sustainable profitibility.
6	Regulatory Bodies	External	Responsibility and authority to ensure compliance to law	Compliance with statutory and regulatory requirements
7	Competitors	External	Provide challenges to our ability.	Healthy competition
8	GOI	External	Govt. has responsibility towards PSUs	Meet MoU goals, implement Govt. policies, Support Govt. initiatices
9	Ministry of Communications	External	Administrative Ministry for ITI Ltd	Reporting and Controlling of ITI Ltd
10	Department of Public Enterprises (DPE)	External	DPE issues guidelines for all PSUs	Compliance to the Guidelines
11	Ministry of Corporate Affairs	External	Issues guidelines for corporate governance	Corporate Governance compliance
12	Ministry of Labour	External	Governs all labour policies for ITI Ltd	Compliance to labour policies by ITI Ltd
13	SEBI	External	Responsibility and authority to ensure compliance to law	Compliance with statutory and regulatory requirements
14	ToT Partners	External	Contribution towards product / service realization, technology partnership	Mutual benefit
15	JV	External	Contribution towards product / service realization, technology partnership	Mutual benefit

Context Analysis Log: Issues List

S. No.	Interested Party	Issue of Concern	Category
1	GOI	MoU goals	Mixed
2	Ministry of Communications	Short term objectives	Mixed
3	Ministry of Communications	Strategic objectives	Mixed
4	Ministry of Communications	Oranizational internal goals	Opportunity
5		Liquidity Damages	Risk
6	Staff / Workers	Delayed payments	Risk
7		GFR compliance	Risk
8	JV	JV	Mixed
9	Customer	Customer Satisfaction	Mixed
10		AMC engagements with railways and payment issue	Risk
11	GOI	Confirmation & reconciliation of balances	Risk
12	GOI	Capex grant	Risk
13	GOI	Change in Govt. policy	Mixed
14	Ministry of Communications	Patents	Opportunity
15	Ministry of Labour	Compliance to Statutory Requirements (e.g. PF, etc.)	Risk
16	Staff / Workers	Employee survey	Risk

Enterprise Risk and Opportunity Register

<Unit Name>

Change History

Document Change History

Version	Date	Completed By	Reason for Change

Instructions

Enterprise Risk and Opportunity Register - Instructions

1. Overview

The Enterprise Risk Register consists of:
Title Page - A cover page for this Risk Register when printed.
Risk Register - A register of all risks identified.

Opportunity Register - A register of all opportunities identified.

Title Page
A cover page for the Enterprise Risk Register when printed.

Risk Register
The Risk Register is used to record identified risks, and assess their likelihood and impact. How the organization will handle each risk is documented as a series of responses. Each response documents an action directed at minimizing the potential negative impact of the risk on the organization's success. The strategy for handling a risk may have one or more responses. These individual actions are then assigned to relevant stakeholders who will be held accountable for their execution.

2. How to Use the Risk Register

The fields on the Risk Register tab are described below. Most fields also have additional help text (red triangle in top right hand corner of column title) in the field comments (hover the cursor over the appropriate column title to see comments).

Risk Register tab

ID	Enter the risk ID number, a sequential number which uniquely identifies each risk
Issue Reference	If the risk relates to an issue documented as part of the Context Analysis (see tab Context Analysis - Issues), provide reference to it. It may be noted that not all risks may be emanating from the Issues identified during the Context
Risk Category	Risks may be identified and grouped under the risk categories and sub-categories defined in the tab Risk Categories. This field is a pull down menu. It will present list of risk categories as defined in the tab Risk Categories. These are: Business Risk / Operational Risk / Environmental Risk / Financial Risk / People Risk / Compliance Risk / Information Technology Risk / Infrastructure Risk / Other Risk
Risk Sub-Category	Risks may be identified and grouped under the risk categories and sub-categories defined in the tab Risk Categories. This field is a pull down menu. It will present different list of risk sub-categories, depending on the chosen risk category.
Risk Description	Enter the description of the risk that is likely to occur
Risk Impact	Describe the impact to the enterprise if the risk occurs
Date identified	The date when either the risk was identified or entered into the risk register
Risk Owner	Person responsible for managing the risk. Typically, this would be the Process Owner of the process in which the risk has been identified.
Status	Choose one of the following possible status conditions:
	Identified - Risk has been identified. Prevention and contingency plans are being developed
	Monitored - Risk has prevention actions identified and contingency plans prepared
	Triggered - Risk has occurred. Contingency plan is being implemented
	Complete - Risk has occurred. Contingency plan is complete. Risk is no longer active
	Obsolete - Risk is obsolete. The time has passed when the risk could have occurred
Risk Treatment Strategy	Enter the appropriate risk treatment strategy as follows: Avoid - Try to avoid / prevent the undesirable risk event from occurring. Transfer - Transfer the risk to someone else (e.g. through Insurance, Outsourcing) Mitigate - Reduce the likelihood and / or impact of the risk. Accept - Accept the consequences of the risk without taking any action.
Likelihood Rating	Choose from 1-Low, 2-Medium, or 3-High, the likelihood of the risk occurring Refer to the tab Likelihood Ratings for details.
Impact Rating	Choose from 1-Low, 2-Medium, or 3-High, the impact to the organization if the risk occurred Refer to the tab Impact Ratings for details.
Risk Score	Do not edit this field. It is a calculated field by multiplying the likelihood rating with the impact rating. This field is then used as the basis to prioritize the risks for attention.
Priority	Do not edit this field. It is a calculated field. Depending on the Risk Score, it would range from Priority 1 (top priority) to Priority 3 (least priority). Refer to the tab Risk Prioritization Matrix for details.

Instructions

Proposed Risk Treatment Actions	Provide details of Risk Treatment Actions. If it is very lengthy, such details could be maintained in an annexure or as a separate document. In such a case, provide reference to the annexure / external document.
Risk Treatment Target Date	Enter the date that the risk treatment will be implemented
Risk Reserve Fund	Enter the amount of money needed to treat the risk effectively.
Risk Approved? (Y / N)	This is an indicator whether the risk has been approved by the appropriate authority. At the unit level, the risk entered in the risk register must be approved by the URMC. At the enterprise level, the risk entered in the risk register must be approved by the ERMSC.
Status Update/Actions	Enter the status of the risk treatment action(s). Prefix updates with date of status update. Keep latest update at the top.

The description of the fields in the Opportunity Register is similar to those described above.

Enterprise Risk Register

ID	Issue Reference	Risk Category	Risk Sub-Category	Risk Description	Risk Impact	Date Identified	Risk Owner	Status	Risk Ttreatment Strategy	Likelihood Rating
R-01										
R-02										
R-03										
R-04										
R-05										
R-06										
R-07										
R-08										
R-09										
R-10										
R-11										
R-12										
R-13										
R-14										
R-15										
R-16										
R-17										
R-18										
R-19										
R-20										

Enter all the risks above this line only. If more lines are needed to be added to the risk register, copy an existing record, insert just above this line and edit it for the new risk.

Enterprise Risk Register

Impact Rating	Risk Score	Priority	Proposed Risk Treatment Actions	Risk Treatment Target Date	Risk Reserve Fund (INR)	Risk Approved? (Y / N)	Status Update / Actions Taken
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						

Total Risk Reserve Fund **0**

Enterprise Opportunity Register

ID	Issue Reference	Opportunity Category	Opportunity Sub-Category	Opportunity Description	Opportunity Impact	Date Identified	Opportunity Owner	Status	Opportunity Treatment Strategy	Likelihood Rating
O-01										
O-02										
O-03										
O-04										
O-05										
O-06										
O-07										
O-08										
O-09										
O-10										
O-11										
O-12										
O-13										
O-14										
O-15										
O-16										
O-17										
O-18										
O-19										
O-20										

Enter all the Opportunities above this line only. If more lines are needed to be added to the Opportunity register, copy an existing record, insert just above this line and edit it for the new Opportunity.

Enterprise Opportunity Register

Impact Rating	Opportunity Score	Priority	Proposed Opportunity Treatment Actions	Opportunity Treatment Target Date	Opportunity Reserve Fund (INR)	Opportunity Approved? (Y / N)	Status Update / Actions Taken
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						
	0						

Risk Categories

Risk Categories	Risk Sub-Categories	Description
Business Risk		
	Concentration Risk	Risk arising from over-dependence (i.e. lack of diversification) on a single customer, industry, product, location, supplier, etc for achieving the goals of the organization.
	Competition Risk	Risk arising from competitors gaining competitive advantage by taking away the organization's market share, customer base, etc.
	Government Policy Risk	Risk arising from changes to the government policies, rules and regulations
	Product Risk	Risk arising from non-viability of the product in a particular market
Operational Risk		
	Project Risk	This may include Project Delay Risk, Project Budget or Cost Overrun Risk, Transportation Risk, SLA Non-Compliance Risk, Penalty Risk
	Quality Risk	Risk arising from the poor quality of product or service, as perceived by the concerned stakeholder (e.g. customer)
	Supply Chain Risk	Risk arising from the delays in supply or non-availability of critical material or equipment
	Technology Risk	This may include Production Failure Risk (/ Equipment Breakdown Risk / Equipment Obsolescence Risk / Maintenance Risk
Environmental Risk		
	Pollution Risk	Risk of polluting the environment
	Disaster Risk	Risk of natural or man-made disaster causing adverse impact on the goals of the organization
Financial Risk		
	Working Capital Risk	Write-Off Risk, Accounts Receivable Risk, Accounts Payable Risk, Cash Flow Risk, Credit Risk, Interest Rate Risk
	Liquidity Risk	Risk that for a certain period of time a given financial asset, security or commodity cannot be traded quickly enough in the market without impacting its market price.
	Fraud Risk	Risk of organization being subjected to fraudulent activity
	Foreign Exchange Risk	Risk arising due to fluctuations in foreign exchange rate of a currency
	Taxation Risk	Changes in tax related policies causing financial outflows. (Risks related to tax compliance are covered under Compliance Risk).
People Risk		
	Skill Gap Risk	Skill Obsolescence Risk / Skill Gap Risk / Skill Mismatch Risk
	Attrition / Offer Decline Risk	Risk arising due to undesirable employee attrition in the organization or due to recruited candidate declining the offer resulting in delays in operations
	Employee Safety Risk	Risk to the physical and mental safety of the employees (what about contract workers?)
	Industrial Relations Risk	Risk arising due to unrest caused by employees or other stakeholders such as general public, suppliers, etc.
	Pandemic Risk	Risk of a pandemic (e.g. COVID-19) causing adverse impact on the goals of the organization
Compliance Risk		
	Statutory Compliance Risk	Statutory Compliance Risk
	Legal Risk	Litigation Risk
Information Technology Risk		
	Information Security Risk	Risk arising due to breach of confidentiality, integrity and availability of the information assets of the organization
	IT Systems Capability Risk	Risk arising due to inadequacy of the IT Systems in terms of capacity, performance, etc.
Infrastructure Risk		
	Infrastructure Security Risk	Risk of encroachment or illegal use of infrastructure assets
	Asset Utilization Risk	Risk arising due to sub-optimal utilization of assets
Other Risk		
		Any risk not falling under any of the above categories may be classified here.

Enterprise Likelihood Ratings

Likelihood Rating	Likelihood Rating Number	Likelihood Rating Description	Likelihood Rating Criteria
High	3	Highly Likely	Likelihood >= 71% and < 100%
Medium	2	Likely	Likelihood >= 31% and <= 70%
Low	1	Less Likely or Unlikely	Likelihood > 0% and <= 30%

Impact Rating	Impact Rating Number	Impact Rating Description	Impact Rating Criteria
High	3	High impact on Revenue and / or Profitability goal or other goals AND/OR	Impact >= 10% (on Revenue / Profitability goal)
		High Impact on Reputation AND/OR	Rate it based on adverse publicity / news affecting the organization
		High Impact on Compliance Obligations	Major Non-Compliance, Severe Penalty (> 5% of annual revenue)
Moderate	2	Moderate impact on Revenue and / or Profitability goal or other goals AND/OR	Impact >= 5% and < 10% (on Revenue / Profitability goal)
		Moderate Impact on Reputation AND/OR	Rate it based on adverse publicity / news affecting the organization
		Moderate Impact on Compliance Obligations	Moderate Non-Compliance, Moderate Penalty (> 3% and <= 5% of annual revenue)
Minor	1	Minor impact on Revenue and / or Profitability goal or other goals AND/OR	Impact < 5% (on Revenue / Profitability goal)
		Minor Impact on Reputation AND/OR	Rate it based on adverse publicity / news affecting the organization
		Minor Impact on Compliance Obligations	Minor Non-Compliance, Minor or No Penalty (< 3% of annual revenue)

Risk Prioritization Matrix			Impact		
			High	Moderate	Minor
			3	2	1
Likelihood	High	3	9 (Priority 1)	6 (Priority 2)	3 (Priority 3)
	Medium	2	6 (Priority 2)	4 (Priority 3)	2 (Priority 3)
	Low	1	3 (Priority 3)	2 (Priority 3)	1 (Priority 3)

Risk Treatment Plan

<Risk ID>

<Unit Name>

Change History

Document Change History

Version	Date	Completed By	Reason for Change

RISK TREATMENT PLAN						
Risk Reference ID in the Risk Register:						
EXISTING CONTROLS						
Existing Control	Challenges/Issues with existing control	Changes proposed in the existing control	Responsibility	Target Completion date	Resource requirement	Budgetary Requirement
					Subtotal - Existing Controls	0
PROPOSED NEW CONTROLS						
New Control	Advantage of the new control	Changes proposed through the new control	Responsibility	Target Completion date	Resource requirement	Budgetary Requirement
					Subtotal - New Controls	0
Signature of Risk Owner				Signature of Enterprise / Unit Risk Officer		

Note:

For completion of Risk treatment actions, the overall responsibility lies with the respective risk owner.

In addition to the risk requirement part, where responsibility for a particular activity or job is mentioned, following details also need to be provided:

Calculations:

Assumptions:

* Each department within ITI will be expected to extend full support and cooperation to the respective Risk Owner in terms of allocating the resources required for successful execution of Risk Treatment Plans.

** The budgeted amount refers to the total planned cost for executing the Risk Treatment Plan.