Risk Management Policy

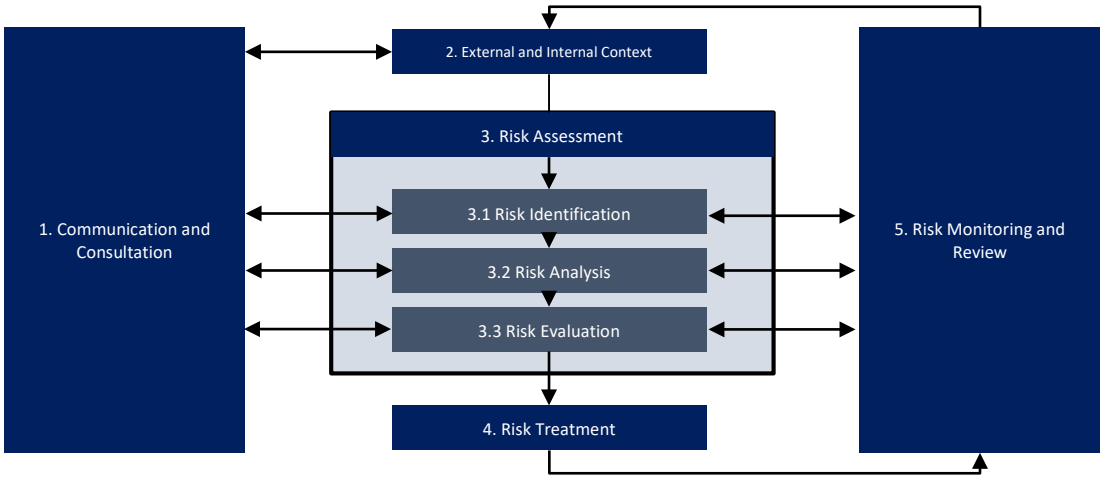
Corporate Office: Club 125, Plot No. A – 3,4,5 Tower A, 4th Floor,
Sector-125, Noida – 201301, UP, India | Tel: +91 120 5057000
Registered Office: M-140, Greater Kailash, Part-II, New Delhi - 110048

CIN No. : L72900DL2012PLC244966
E-mail: help@rategain.com
Website: www.RateGain.com

Risk Management Policy

I. Risk Management Process / Plan

ERM process is the systematic application of management policies, procedures, and practices to the activity of communicating, consulting, and establishing the context for ERM in the Company. The ERM process comprising of risk assessment, risk treatment and risk monitoring applies across the organizational lifecycle.



1. Communication and consultation

Communication and consultation are intended to facilitate regular exchanges of information, considering confidential aspects. Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Effective external and internal communication and consultation is essential to ensure that personnel responsible for implementing the risk management process and stakeholders understand issues relating to risk, its causes, consequences, and the measures being taken to treat it.

2. External and Internal context

Risks may arise from factors that are external to the organization. Further, to pursue objectives, the organization might make internal changes that could result in exposure to risks. An effective ERM process takes cognizance of both external and internal context in which the Company operates. This entails understanding the external and internal context of the Company to ensure that risks identified are aligned to the same.

2.1 Considerations of external context

The following are indicative factors that need to be considered/ understood from an external context perspective:

- New/ changes in policies or regulations that may affect the business decisions
- Competitive landscape and position taken by competitors
- Supplier, partners, alliances
- Political scenario in India as well as in the countries where the Company has business interests
- Economic condition in the countries / region of operation

- Social factors that may affect the decisions pertaining to a project
- Technological changes applicable to each business segment

2.2 Consideration of internal context

The following need to be considered/ understood from an internal context perspective:

- Strategy and objectives of the company
- Inherent strengths and weaknesses / vulnerabilities
- Organization structure and expected roles & responsibilities
- Values & beliefs
- Profile of people (qualification/ experience and its relevance to their role)
- Performance appraisal mechanisms
- Systems and processes
- Supervision and monitoring mechanisms

3. Risk Assessment

Risk assessment comprises of:

- Risk identification
- Risk analysis and
- Risk evaluation

Risk assessment is intended to:

- Proactively identify risks considering the external and internal context
- Provide the Company with an improved understanding of risks that can affect achievement of objectives and the possible business impact of manifestation of risks
- Evaluate the design adequacy of existing response systems
- Enable risk prioritization and further treatment

3.1 Risk identification

Risk identification is the mechanism of identifying exposure to uncertainty across the Company. This involves assessment of the external context within which the Company operates, as well as the internal context of the Company.

As part of risk identification, a comprehensive list of risks is generated based on events (historical and anticipated) which may prevent, degrade, accelerate, or delay the achievement of objectives. It shall also include risks associated with not identifying / evaluating opportunities pursuant to the organization's strategic, project or business objectives, otherwise being pursued by competing organizations.

The risk causes, source, events, situations, or circumstances which could have a material impact on the objectives of the company shall also be identified during this phase.

Risks once identified shall not be deleted. In case a risk becomes irrelevant, the status of the risk shall be updated to reflect the same.

Risk identification is an ongoing activity. It shall be performed by each employee during the course of his work and particularly at the time of any significant decision, initiation of

opportunity, during product development and execution and periodically during the life of every operating asset. While the CRO shall assist in risk identification, it is the responsibility of each functional owners to identify risks.

Risk identification involves identifying potential sources/ root cause of risk events. The purpose of identifying potential root causes is to give direction to risk intervention measures. The fact that one risk might have multiple root causes also needs to be considered. As a part of the risk identification process, it is also important to understand which of the business drivers are impacted by the materialization of a risk or any of its root causes.

Techniques of risk identification

The following risk identification techniques can be deployed to enable focused risk identification:

- Checklists
- Preliminary hazard analysis
- Structured interview and brainstorming
- Root cause analysis (single loss analysis)
- Scenario analysis
- Business impact analysis

3.2 Risk Analysis

Risk analysis refers to the process followed to comprehend the nature of risk and determine the level of risk. Risk analysis is intended to provide inputs for risk evaluation.

Risk analysis shall be performed for each risk identified. The onus of risk analysis is with the risk identifier, who may choose to consult with the functional head and/or CRO for this purpose. Based on the results of the analysis, appropriate action shall be taken (risk evaluation and risk treatment).

Risk analysis involves consideration of:

- Likelihood of risk
- Time to manifest
- Impact of risk

A. Identified Risks:

- Functional Heads while reviewing and updating the Risk Register, shall identify the key risks (along with the mitigation plan) for the purpose of reporting to CRO on quarterly and/or annual basis. This report to CRO shall also indicate any policy deviations, failure of existing mitigation plans and other major issues, if any, faced during the period.
- CRO shall review the report of the functional heads and may identify additional key risks (along with the mitigation plan), in consultation with functional heads, for the purpose of reporting to RMC on a half yearly basis. This report to RMC shall also indicate any policy deviations, failure of existing control measures and other major issues, if any, faced during the period.
- RMC shall review the report of CRO and suggest directions, if required. Further it shall also escalate key risks, etc. as deemed fit, to the Audit Committee and/or Board annually or earlier if need arises.

- Audit Committee and/or Board shall review the RMC's report and suggest directions, if any.

The Quarterly risk review report includes:

- Risk rate movements
- New risks identified (key and non-key) along with mitigation plan
- Status of implementation of mitigation plan

The half-yearly and/or annual risk review report includes:

- Compiled list of new key risks identified
- Prioritized list of key risks
- Root causes and mitigation plans for key risks
- Effectiveness of mitigation plans for existing key risks

The CRO shall communicate the directions of RMC/AC/BOD, if any, to Functional Heads.

B. Status of Implementation of Mitigation Plans:

The status of implementation of the approved Mitigation plans shall be reviewed by the Functional Heads and reported to CRO on a quarterly and / or annual basis.

To visually depict the prioritization, a "heat map" (graphical representation of impact and likelihood) maybe used based on the risk analysis (i.e., Likelihood * Impact) wherein each risk will be plotted on the "heat map" based on its relative likelihood and impact. The placement of the risks on the "heat map" will indicate the risk zone (High/ Medium/ Low) for each of the respective risks. The heat map shall also form the basis of escalation as and when new risks are identified.

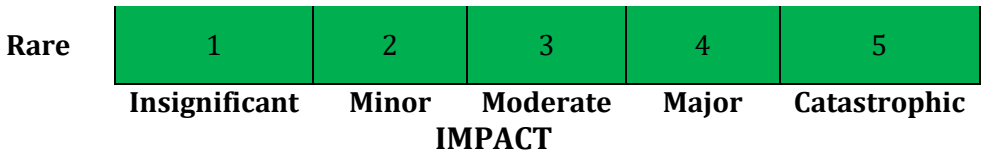
A five-by-five matrix shall be used for measuring likelihood and impact. The risk shall be evaluated as:

Risk Measurement: Likelihood * Impact

It is important to note that a single risk may impact a number of impact parameters. In such a scenario, the risk shall be evaluated for all impacts and the highest score shall be used for escalation and evaluation purposes.

The risks assessed can be placed on a "heat map" which is a graphical representation of the impact and likelihood.

LIKELIHOOD						
	Most Probable	5	10	15	20	25
	Probable	4	8	12	16	20
	Possible	3	6	9	12	15
	Unlikely	2	4	6	8	10



The overall risk measurement will be assessed as below:

Likelihood * Impact (Range)	Risk Zone
Score – less than 8	Low
Score – greater than or equal to 8 but less than 15	Medium
Score – greater than or equal to 15	High

3.3 Risk Evaluation

Risk evaluation is the process to determine whether the risk and/ or its magnitude is acceptable or tolerable.

The intent of risk evaluation is to:

- Enable escalation to the appropriate level of management as per risk measurement criteria
- Prioritize for treatment implementation

Risk evaluation helps ensure appropriate resource allocation for the purpose of risk treatment and channeling of management attention towards risks of significant concern.

Risk evaluation shall be done individually by functional heads and collectively by CRO.

a) Risk escalation

A critical element of ERM is an effective system of escalation which ensures that specific issues are promptly communicated to relevant authorities. In the context of the Company, escalation may stem from one or more of the following:

- Identification of new risks at Risk Owners/RateGain level
- Change in impact/ likelihood of identified risks causing a change in the risk evaluation
- Unforeseen contingencies

It is to be noted that at each level of escalation, the risk shall be reassessed so that only the key risks are filtered upwards on a timely basis.

b) Risk prioritization

The ranking of risks in terms of net potential effect provides management with some perspective of priorities. This should assist in the allocation of capital and resources in the business. Although the scales of quantification will produce an automated ranking of risks, management may choose to raise the rank of certain risks for other reasons. This may be justified because of non-financial influences such as media implications, social responsibilities, or regulatory pressures. The ranking of risks should be shaped by strategic and business objectives. The prioritized risks must be compared with the risk appetite and all risks falling beyond the acceptable appetite must be short listed for risk treatment.

4. Risk treatment

Risk treatment involves selecting one or more options for managing risks and implementing such action plans. This phase of the ERM process is intended to:

- Understand existing controls/ mitigation mechanisms in place for managing risks
- Develop a new risk treatment plan
- Assess the effectiveness of such treatment plans

For the purpose of risk treatment, risk owners may consider various options (as indicated below) for risk treatment:

- **Accept Risk** - Retaining the risk by informed decision
- **Reduce Risk** - Changing the likelihood or consequences of risk by instituting new control/ monitoring activities
- **Share/Transfer Risk** - Sharing the risk with another party or parties (e.g.: insurance, back-to-back warranties etc.)
- **Avoid / Eliminate Risk** - by not initiating or continuing with the activity / source giving rise to such risk

Risk treatment can be a choice from the above or a combination of multiple options. For example, a combination of partially sharing the risk (through insurance) and partially accepting the risk can be the chosen treatment for a risk.

The choice of an appropriate treatment option must consider balancing the costs and efforts of its implementation against the benefits derived.

Further, the cost of controlling and mitigating the risk should not exceed the magnitude of risk except for regulatory and compliance.

Steps for risk treatment:

- Evaluate the mitigations in place for identified risks
- Evaluate control requirements for risk treatment
- Verify and evaluate the controls currently in place
- Identify, evaluate and review the risk protection measures in place to respond to the consequences of risk events
- Take decisions on the acceptability of identified risks and controls
- Document action plans for risk mitigation
- Use the outputs of risk assessments for budgeting and capital allocation processes

4.1 Residual Risk

The threat a risk poses after considering the current mitigation activities in place to address it and can be an important metric for assessing overall risk appetite. A risk tolerance range for minimum and the specific maximum risk is typically set by the committee responsible for risk management oversight and accepted by the board of directors.

This means that if a risk's impact on the organization, multiplied by its likelihood of occurring, multiplied by the effectiveness of current mitigation activities falls outside of the level deemed acceptable, then the risk factor is out of tolerance.

Business process owners must then adjust risk mitigation activities, procedures, or controls to keep the residual risk within the defined risk tolerance.

4.2 Managing Residual Risk

Managing residual risk comes down to the organization's willingness to adjust the acceptable level of risk in any given scenario. For any residual risk present, organizations can do the following:

- **Nothing -** Assuming the residual risk is below the acceptable level of risk in any endeavor, organizations can simply accept that the implemented controls have proven effective enough to reduce the risk to an acceptable level.
- **Update or increase controls implemented -** In case where the residual risk is still above an acceptable risk level, new or modified controls and processes may be needed to reduce the inherent risk to a level that is deemed acceptable.
- **Evaluate controls vs. mitigation costs to decide -** In case where the residual risk is still beyond the acceptable level of risk and the cost of the needed controls and countermeasures is too high, organizations may need to accept the risk, regardless of what residual risk remains.

5. Risk Monitoring and Review

Risk monitoring, review and reporting are critical components of the ERM process. The intent of risk monitoring and review along with their respective treatment plans is to:

- Analyze and track events, changes, trends which affect identified risks
- Detecting changes and assessing the impact of changes to risk appetite, risk portfolio, risk treatment plans
- Ensure that risk treatment mechanisms are effective in design and operation

Risk monitoring shall be conducted by each functional owners on an ongoing basis, for identified risks, in order to track the status of treatment plans and consequently update changes to risk profiles.

Risk reviews shall be conducted to enable continuity of the ERM process. Risk reviews entail the reassessment of all risks recorded in the risk registers along with new/ emerging risks to ensure concurrence and relevance of risks and their treatment. Risk reviews will be carried out by functional owners at a minimum on a quarterly basis.

The calendar for monitoring/ reviews is provided below:

Activity	Timing
Risk monitoring by Functional Owners	Ongoing basis
Risk reporting by Functional Owners to CRO	Quarterly
Key risk review by Risk Management Committee	Half-yearly
Key risk review by BOD	Annual

II. Current State Assessment of ERM - Approach and Methodology

Step 1: Formulation of questionnaire and finalization of list of respondents'

- Draft questionnaire based on the 3 pillars of the Enterprise Risk Management (ERM) process: Risk Governance, Risk Infrastructure and Risk Ownership.
- Shortlist the list of respondents in consultation with the management who were to give their feedback during the current state assessment process; and
- Select set of risk related documentations e.g., risk policy, risk registers, reports which needs to be reviewed to gain an independent view on the maturity of the existing ERM program.

Step 2: Collate questionnaire responses and undertake walkthrough of documentation

- Collate the responses provided by the designated respondents.
- Perform walk-through on the risk related documentation to independently assess the current state assessment of the existing ERM program; and
- Gather feedbacks by way of interactions with key stakeholders about the risk management process of the organization

Step 3: Report the results

- Consolidate insights gathered through the feedbacks provided by the respondents as well as the results of documents walk-through.
- Feedbacks provided by the respondents are assigned numerical values (NV) to derive scores:
  - Strongly Disagree (1 Point)
  - Disagree (2 Points)
  - Neither Agree nor Disagree (3 points)
  - Agree (4 Points)
  - Strongly Agree (5 Points)
- The score for an individual question / section is derived by taking "Arithmetic Average" i.e.

$$\frac{(\text{no. of Strongly Agree X5}) + (\text{no. of Agree X 4}) + (\text{no. of Neither Agree/Disagree X3}) + (\text{no. of DisagreesX2}) + (\text{no. of Strongly Disagree X 1})}{\text{Sum total of no. of responses}}$$

- Basis the importance of the question, specific weights are assigned.
- Based on the 5 stages of the Risk Maturity Model, conclusion shall be made on the current maturity state of the company.

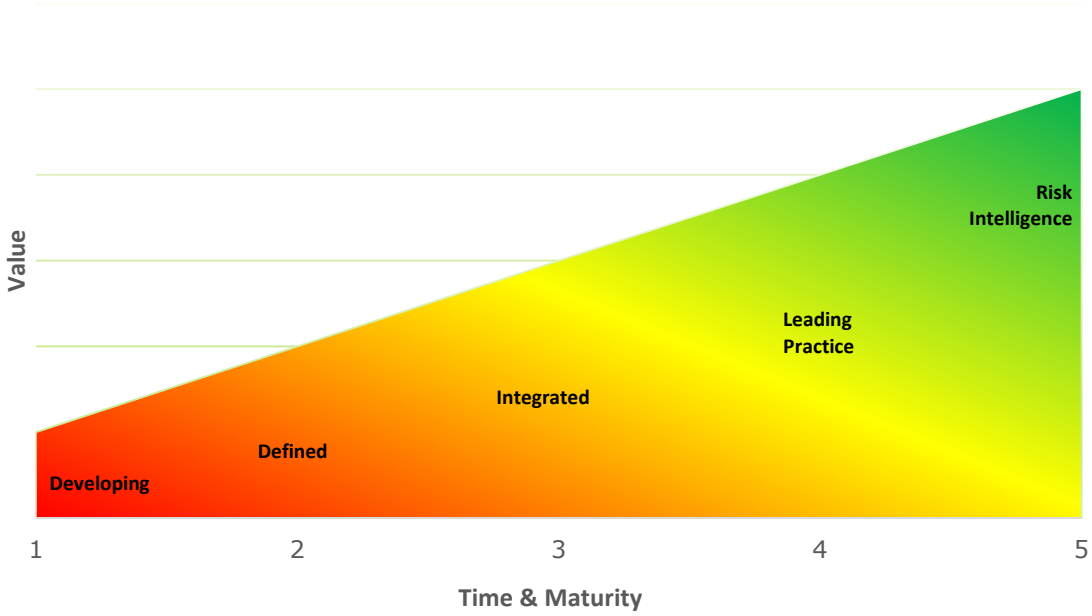
3 pillars of the Enterprise Risk Management (ERM) process, along with Current State Assessment parameters

Risk Governance Oversight of risk	**Definition &common framework** ✓ Concepts of	**Roles and Responsibilities** Risk management	**Transparency** Board and Audit Committee have appropriate	**Oversight/Tone at the top** The top level, Risk Governance directs

management by Leadership and the Board.	value preservation and value creation ✓ Consistent usage of common framework	related roles are uniquely delegated across the organization.	transparency into risk management.	Risk the Intelligent Enterprise. It defines parameters of acceptable risk, monitors strategic alignment, sets overall risk and management expectations.
Risk Infrastructure and Management People, Process and Technology to report, measure and monitor risk.	**Common Risk infrastructure** Common Infrastructure used throughout the organization to support business and functions in performance of their risk related responsibilities.	**Executive Management Responsibility** Primary responsibility of designing, implementing, and maintaining an effective risk program.	**Objective Assurance and Monitoring** Functions tasked to provide objective assurance as well as monitor / report on the effectiveness of the organization's risk program.	**People / Process / Technology** The middle level, an infrastructure that consistent supports risk management approaches throughout the organization is essential to the ability to give executive management an enterprise - wide view of risk
Risk Ownership Risk Ownership defined across the three lines of defense within the control framework.	**Risk Identification & Evaluation** ✓ Identification of potential risks pertaining to constituent function groups ✓ Assessing impact and likelihood of risks for risk prioritization	**Risk Response** Formulate appropriate risk response strategies (mitigation plans) considering criticality of risks and establishing ownership for risks.	**Monitoring & Review** ✓ Monitor risks and report to enterprise risk group (risk committee) ✓ Ensure adequate communication and training	**Risk Management Cycle** The bottom level, Risk Ownership is what risk governance relies upon. It includes all the functions' and business segments' responsibilities with regard to managing risks in accordance with the organization's appetite.

III. ERM Maturity Model

Maturity of the risk management program measured across five levels which reflect distinct risk management related characteristics.



Developing	Defined	Integrated	Leading Practice	Risk Intelligence
Activities are unstructured, uncoordinated, and undocumented, or they may be absent. No overreaching philosophy / objectives defined.	Most business units function independently. Activities are either not applied consistently across business units or may be in development but are not yet finalized.	Activities are implemented consistently across the enterprise and are correlated and aggregated across risk types (categories) and business units and encompasses most risk types.	Risk is built into decision making. Selectively seize opportunities because of ability to exploit risks	Uses predictive analytics and data driven technologies to automate processes, generate insights and enable risk-intelligent decision making.
✓ Depends primarily on individual capabilities, and skill set ✓ Independent risk and management activities.	✓ Implementation of additional controls based on identified risk ✓ Reporting on risk exposure	✓Common framework, program statement, policy. ✓Routine risk assessments. ✓Communication of key strategic risks to the Board.	✓Coordinated risk management activities across silos. ✓Contingency plans and escalation procedures.	✓Embedded in strategic planning, capital allocation, product development, etc. ✓Early warning risk indicators. ✓Linkage to performance

✓ Limited focus on the linkage between risks.	✓Disparate monitoring and reporting functions ✓Limited alignment of risk to strategies.	✓Executive/Steering Committee. ✓Knowledge sharing across risks functions. ✓Functions have ownerships of risks within operations.	✓Enterprise-wide risk monitoring, measuring, and reporting. ✓Technology implementation. ✓Risk management training.	measurement/ incentive. ✓Risk modelling/scenarios. ✓Industry benchmarking.

IV. Document Management

The ERM framework is owned by the CRO. Changes to the document need to be processed through the owner and require the consensus of the RMC / board for approval.

The framework shall be reviewed bi-annually to ensure that the intent of the same and its covenants are relevant to the company and its entities.

The CRO shall ensure that updates to the framework are communicated across the organization and shall also be responsible for promoting risk awareness across the company. The CRO may use tools, workshops, newsletters, formal training sessions, and undertake other initiatives as deemed required for this purpose.

Record Retention

For the purpose of ensuring traceability of ERM activities, documentation such as risk registers, periodic reports, questionnaires etc. shall be maintained in physical or electronic form and retained for eight (8) years or as per Company's Corporate Record Retention Standards.
Records, both physical and electronic, at an enterprise level shall be maintained by the CRO on behalf of the Company/ Board of Directors.

V. Business Continuity Plan (BCP)

Business Continuity Plans (BCP) are required to be defined for risks corresponding to High Impact and High Velocity to enable rapid response to address the consequence of such risks when they materialize. Business Continuity Planning shall be part of Internal Controls and Crisis Management for areas like information technology function, customer success, human resource, project management, etc. The internal crisis management team (which ideally consist of representatives from each critical business process) shall be responsible for laying out crisis response mechanism, communication protocols, and periodic training and competency building on crisis management. The Crisis Management team shall also conduct periodic disaster recovery mock drills to ensure that the organization is prepared to manage any crisis event quickly for business continuity.