RISK MANAGEMENT POLICY AND PROCEDURES

Version 4.0

GAIL (India) Limited

(A Government of India Undertaking)

Contents

INTRODUCTION

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their business objectives. The effect this uncertainty has on an organization's objectives is “RISK”. In recent times all sectors of the economy have shifted focus towards the management of risk as the key to making organizations successful in delivering their objectives while protecting the interests of their stakeholders. Risk may be defined as events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization’s business objectives. The exposure to the consequences of uncertainty constitutes a risk.

Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so. Simply put, companies make money by taking intelligent risks and lose money by failing to manage risk intelligently.

Risk management is a holistic, integrated, structured and disciplined approach to managing risks with the objective of maximizing shareholder’s value. It aligns strategy, processes, people & culture, technology and governance with the purpose of evaluating and managing the uncertainties faced by the organization while creating value.

With the vision to integrate risk management with the overall strategic and operational practices, an Enterprise Risk Management Framework has been established by GAIL (India) Limited, as a comprehensive set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

DEFINITIONS

Risk

Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. The exposure to the consequences of uncertainty constitutes a risk.

Risk Management

Risk management Process can be defined as the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risk Register

A prioritized risk register highlighting the key risks for the unit where the Total Risk Score is greater than or equal to 12 and/or the Impact is rated as Very High (5)

Risk Database

The risks have been classified based on the Business Units and Functions. Repository of all risks facing GAIL India Ltd. categorized as High, Medium or Low based on the impact and likelihood ratings.

Trigger Events

Events or conditions that could lead to the risk

Impact

The degree of consequences to the organization should the event occur. [Refer to impact scale criteria definitions – Appendix I]

Likelihood

The likelihood of the event occurring expressed as an indicative annual frequency. [Refer to likelihood scale criteria definitions – Appendix I]

Consequence

Potential resulting events that could be affected by the key group risk.

Risk Source

Element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Rating

The relative rating determined from the risk score derived from qualitative analysis of impact and likelihood. Categorized as High, Medium or Low. [Refer to Risk Rating definitions – Appendix I]

Risk Management Committee (RMC)

Risk Management Committee is Board nominated committee consisting of All Functional Director, Head of Treasury and Chief Risk Officer (CRO). Currently the RMC is headed by Director (Marketing).

1.0 PURPOSE OF THE POLICY

- The policy forms part of GAIL's Internal control & Governance arrangements.
- The policy explains GAIL's approach to risk management, documents the roles & responsibilities of the Board/ Audit Committee/ Corporate Level Risk Steering Committee/ Chief Risk Officer/ Risk owners etc.
- It also outlines the key aspects of the risk management process & identifies the reporting procedures.
- This policy shall operate in conjunction with other business and operating / administrative practices.

1.1 POLICY STATEMENT

GAIL (I) ltd, is committed to develop an integrated Risk Management Framework :

- To achieve the strategic objective while ensuring appropriate management of risks
- To ensure protection of stake holders value
- To provide clear & strong basis for informed decision making at all levels of the organization
- To strive towards strengthening the Risk Management System through continuous learning & improvement

Every employee of the company is recognized as having role in risk management for identification of risk to treatment and shall be invited & encouraged to participate in the process.

There will be a Corporate Level Risk Steering Committee to determine Key Risks, communicate Policy, objectives, procedures & guidelines and to direct & monitor implementation, practice & performance throughout the Company.

The Audit Committee & the Board will review the policy & procedures periodically.

1.2 OBJECTIVES OF THE POLICY

The prime objective of this Risk Management Policy and Procedure is to ensure sustainable business growth with stability and establish a structured and intelligent approach to Risk Management at GAIL (India) Limited. This would include the process for development and periodic review of the unit-wise Risk Registers and Databases in order to guide decisions on business risk issues. This would promote a proactive approach in analysis, reporting and mitigation of key risks associated with the business in order to ensure a sustainable business growth.

The specific objectives of the Risk Management Policy are:

1. To establish a risk intelligence framework for the organization;
2. To establish ownership throughout the Organization and embed risk management as in integral part of the business rather than a stand-alone system
3. To help the decision makers of the organization explicitly take account of uncertainty, the nature of that uncertainty, and work towards a solution to address it

4. To ensure that all the current and expected risk exposures of the organization are identified, qualitatively and quantitatively evaluated, analyzed and appropriately managed
5. To enable compliance with the relevant legal and regulatory requirements and international norms
6. To assure demonstrable achievement of objectives and improvement of financial stability of the organization

1.3 SCOPE & EXTENT OF APPLICATION

The policy guidelines are devised in the context of the present business profile, future growth objectives and new business endeavors/ services that may be necessary to achieve the goals & the emerging global standards & best practices amongst the comparable organizations. This policy covers all the events with in the company & events outside the company which have a bearing on the company's business.

2.0 THE RISK MANAGEMENT FRAMEWORK

Risk management will protect and add value to the organization and its stakeholders through supporting the organization's objectives by improving decision making, planning and prioritization by comprehensive and structured understanding of business activity, volatility and project opportunity/threat.

It will provide a framework that enables future activity to take place in a consistent and controlled manner. The framework will help in creating an environment in which risk management is consistently practiced across the Company and where Management can take informed decisions to reduce the possibility of surprises.

The components of risk management are defined by the company's business model and strategies, organizational structure, culture, risk category and dedicated resources. An effective risk management framework requires consistent processes for assessment, mitigation, monitoring and communication of risk issues across the organization. Essential to this process is its alignment with corporate direction and objectives, specifically strategic planning and annual business planning processes. Risk management is a continuous and evolving process, which integrates with the culture of the Company.

An effective Risk Management Framework comprises of:

- Risk management process; and
- Risk management organization structure

Risk management Process can be defined as the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risk Management Organization Structure: The risk management process has to be supported by a risk management structure which primarily comprises of:

- Team structure of the Risk Management Function
- Roles and Responsibilities
- Risk management activity calendar

2.1 THE RISK MANAGEMENT APPROACH AT GAIL (INDIA) LIMITED

GAIL (India) Limited has adopted a comprehensive Enterprise Risk Management approach to identify and manage risks at the overall entity level. The risk methodology adopted has the following two facets to it:

A **"Top-Down"** system, whose objectives are to distill insights and provide clarity on the **KEY RISKS** or the big best shaping company performance, support risk-informed decisions at the Executive Committee levels, ensure a risk dialogue among the management team and enable proper risk oversight by the Board.

A **"Bottom-Up"** system whose objectives are to ensure a comprehensive risk identification and prioritization of important risks, define and follow risk policies and processes that control daily decision making throughout the company and ensure a robust risk culture company-wide.

Top-down ERM

Under this approach, the process / operations level risks have been identified. Risk registers and databases have been created for identified risks along with mitigation plans. From the process level risk registers, entity level top risks have been identified to articulate key strategic and business risks applicable to the Company.

Risk Database: Repository of all risks facing GAIL India Ltd. categorized as High, Medium or Low based on the impact and likelihood ratings. The risks have been classified based on discussions with Business Unit heads and Functional Directors.

Risk Register: Prioritized list of risks that are either high on a multiply product of probability and impact or high on impact (low on probability). Refer to Appendix I for the risk rating matrix.

3.0 RISK MANAGEMENT PROCESS

Effective risk management process requires continuous & consistent assessment, mitigation, monitoring and reporting of risk issues across the full breadth of the enterprise. Essential to this process is a well-defined methodology for determining corporate direction and objectives. The risk management framework adopted by GAIL is mapped as per the ISO Standard 31000: Risk Management - Principles and guidelines and is in-line with recommendations of The Committee of Sponsoring Organizations of the Treadway Commission ("COSO"). Hence, an enterprise wide and comprehensive view will be taken of risk management to address risks inherent to strategy, operations, finance and compliance and their resulting organizational impact.

The risk management process adopted by GAIL (India) Ltd. has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:

- Establishing the Context
- Risk Assessment (identification, analysis & evaluation)
- Risk Treatment (mitigation plan)
- Monitoring, review and reporting
- Communication and consultation

[Refer figure 1 below for detailed flow of the risk management process]

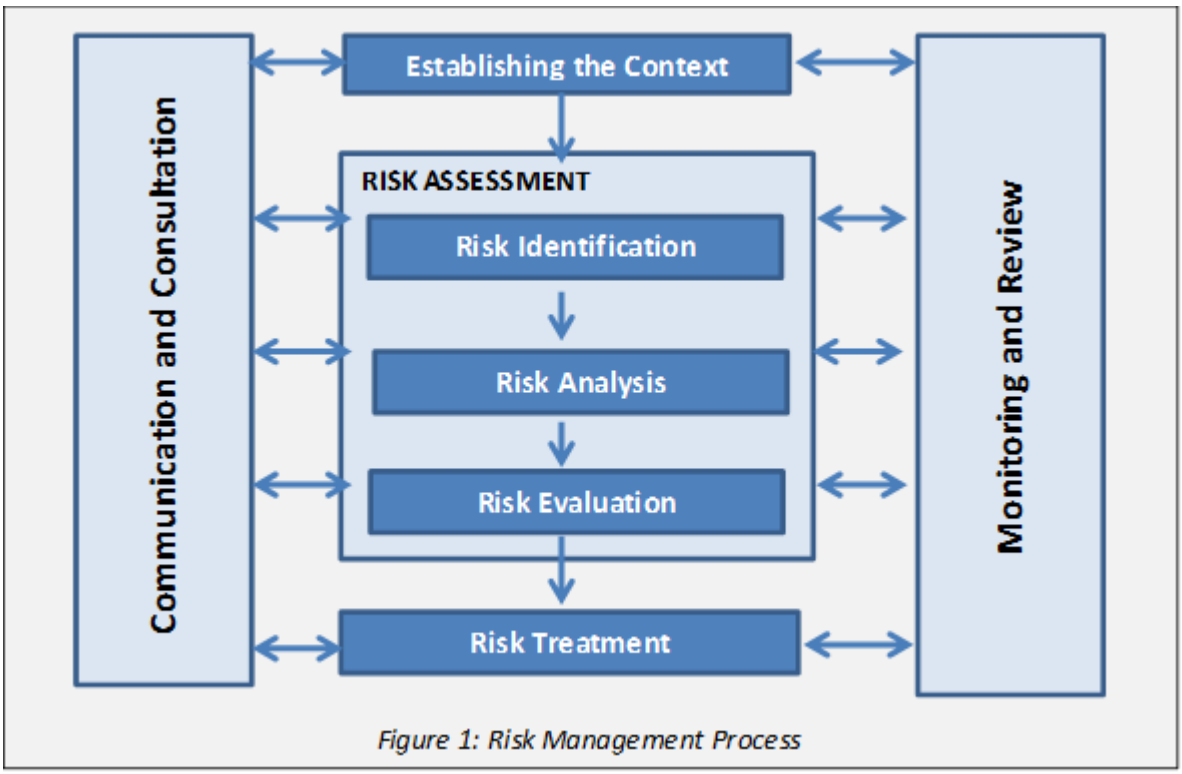


Figure 1: Risk Management Process

3.1 Establishing the Context

Articulate the objectives and define the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process**.**

Establishing the External Context

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, perceptions and values of external stakeholders

Establishing the Internal Context

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way risks will be managed

It is necessary to understand the internal context. This can include, but is not limited to:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- The relationships with and perceptions and values of internal stakeholders; the organization's culture;
- Information systems, information flows and decision making processes (both formal and informal);
- Standards, guidelines and models adopted by the organization

3.2 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

3.2.1 Risk Identification

Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself. This stage involves identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

3.2.2 Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk
- the trigger events that would lead to the occurrence of the risks
- the positive and negative consequences of the risk
- the likelihood that those consequences can occur

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

3.2.3 Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties, other than the organization, that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

[Refer Appendix I for details of the risk criteria definitions required for analyzing risk impact and likelihood]

3.3. Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;

- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:

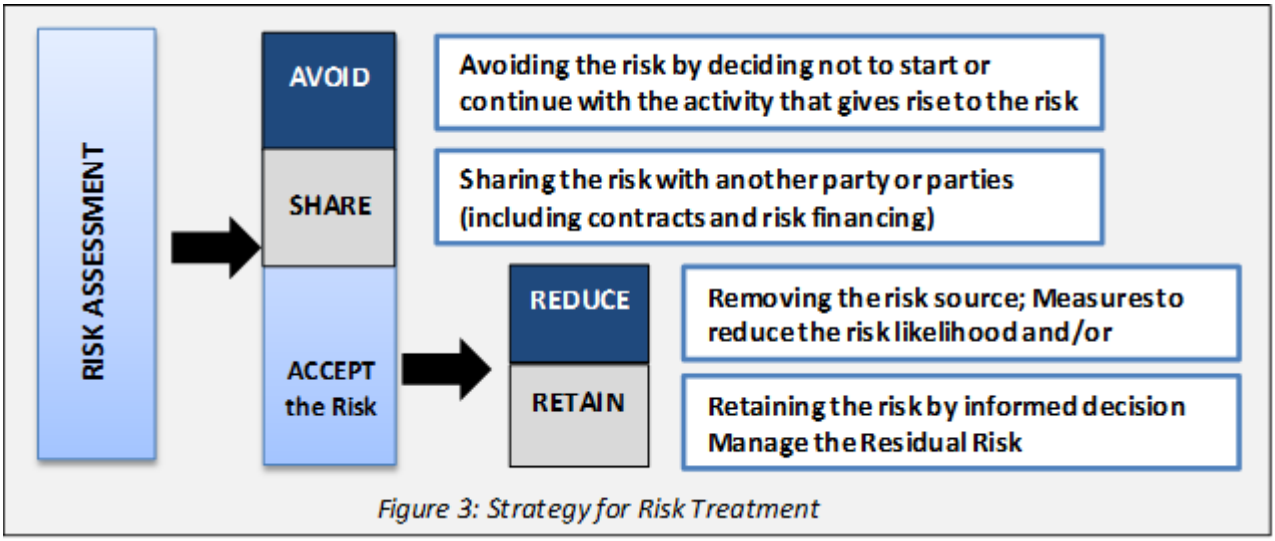


Figure 3: Strategy for Risk Treatment

1. **Avoidance (eliminate, withdraw from or not become involved)**
   As the name suggests, risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. **Reduction (optimize - mitigate)**
   Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

3. **Sharing (transfer - outsource or insure)**
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk

4. **Retention (accept and budget)**
   Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

3.4. Monitoring and review

In order to ensure that risk management is effective and continues to support organizational performance, processes shall be established to:

- Measure risk management performance against the key risk indicators, which are periodically reviewed for appropriateness
- Periodically measure progress against, and deviation from, the risk management plan
- Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed
- Periodically review the effectiveness of the risk management framework.
- Structured scientific and analytical tools may be used for this purpose.

3.5 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required

4.0 RISK REPORTING

Reporting is an integral part of any process and critical from a monitoring perspective. Results of risk assessment need to be reported to all relevant stake holders for review, inputs and monitoring.

Approach for Implementation at GAIL (India) Limited:

A. The **Risk Unit Owners** would be required to prepare unit level risk evaluation reports on a quarterly and annual basis and submit the same on Risk Portal.

Quarterly Risk Register Review Report

The Risk Unit Owners and the Site Level Risk Steering Committee shall review the Risk Registers and identify any emerging/new risk and the existing control to mitigate that risk. They must ensure robustness of design and operating effectiveness of existing mitigating controls. If required, re–rate (existing risks)/rate (emerging risks) and prepare, implement action plan for risk treatment in situations where the existing controls are inadequate.

The Quarterly Risk Register Review Report shall include:

- Risk rate movements, if any, along with reasons for changes in the impact and/or likelihood ratings
- New key risks identified, if any, along with risk criteria ratings and mitigation plans
- Status of the implementation of mitigation plans and reasons for any delays or non-implementations

The Risk Unit owner will be responsible for preparing and consolidating the report and the same shall be reviewed by the Site Level Risk Steering Committee. Approval sign-off by the Site Officer In-Charge (OIC) shall be taken and the report will be shared with the Office of CRO by 10th day following the quarter end.

Post the review and re-rating of the risks in Risk Register, if the Risk Score (factor of impact and likelihood) becomes less than 12 and/or the Impact is rated below 5 (Very High) for a risk existing in Risk Register, **the same risk shall move to Risk Database**.

Annual Risk Database Review Report

The Risk Unit Owners shall review the respective Risk Database annually and evaluate if any changes are requisite to the impact and likelihood assigned to the risks and, re-rate the risks if applicable as per the guidelines and ensure effectiveness of design and operating effectiveness of existing mitigating controls.

The Annual Risk Database Review Report shall include:

- Risk rate movements, if any, along with reasons for changes in the impact and/or likelihood ratings
- New key risks identified, if any, along with risk criteria ratings and mitigation plans
- Status of the implementation of mitigation plans and reasons for any delays or non-implementations

The Risk Unit owner will be responsible for preparing and consolidating the report and the same shall be reviewed by the Site Level Risk Steering Committee. Approval sign-off by the Site Officer In-Charge (OIC) shall be taken and the report will be shared with the Office of CRO by 45th day following the financial year end.

Post review and re-rating of risk in Risk Database, if the factor of impact and likelihood becomes greater than or equal to 12 and/or the Impact is rated as Very High (5), **the same risk shall move to Risk Register**.

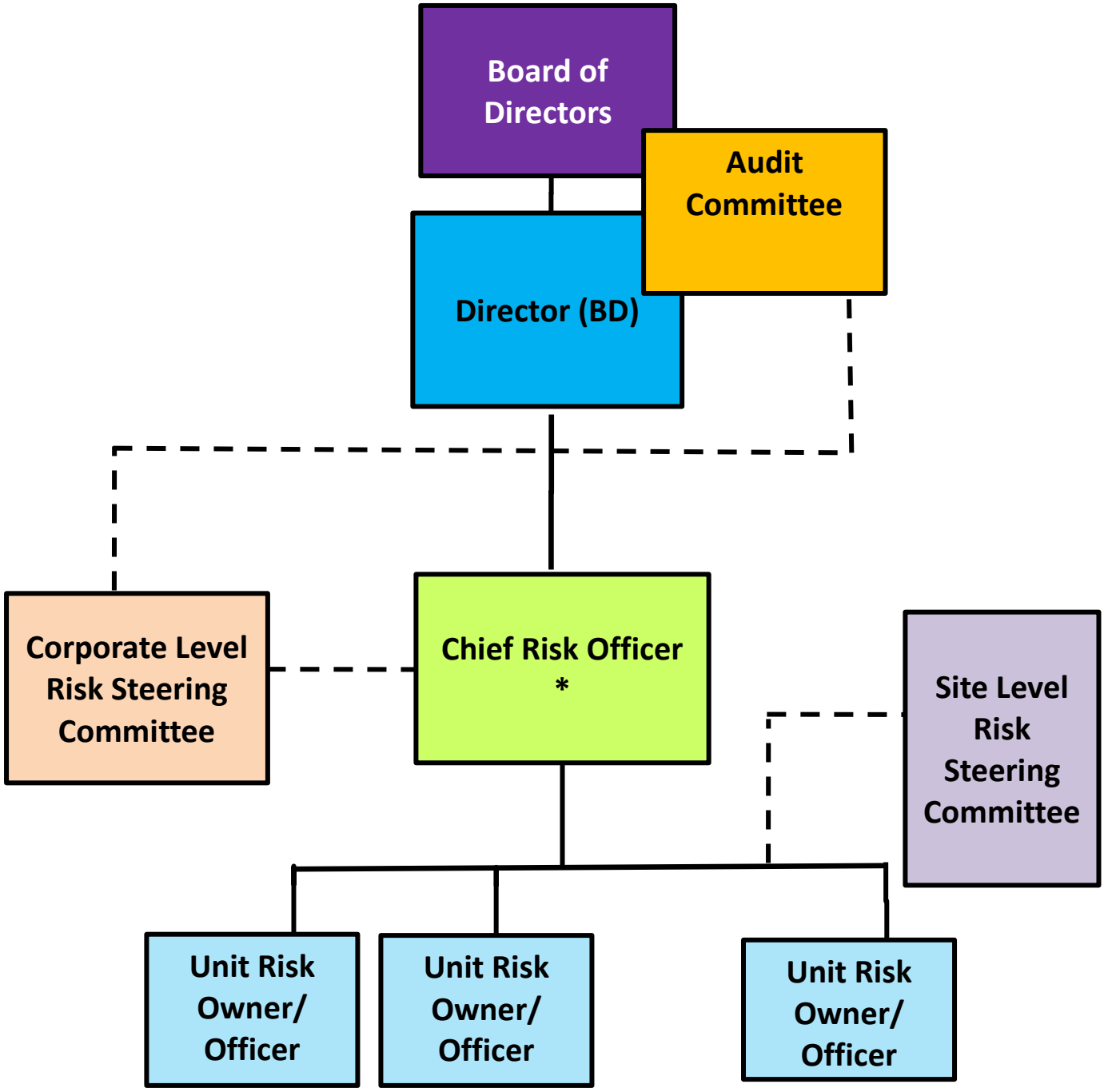
[Refer Appendix II for all the reporting formats]

B. The **Office of CRO** *[Refer Section 5.1 for detailed roles and responsibilities]* would be required to prepare on a quarterly basis a report for the Corporate Level Risk Steering Committee detailing the following:
   - List of applicable risks for the business, highlighting the new risks identified, if any and the action taken w.r.t the existing and new risks;
   - Prioritized list of risks highlighting the Key strategic and operational risks facing GAIL
   - Root causes and mitigation plans for the Key Risk
   - Status of effectiveness of implementation of mitigation plans for the Key Risks identified till date

C. The **Corporate Level Risk Steering Committee** would be required to submit report to the Audit Committee on a quarterly basis the following:
   - An overview of the risk management process in place;
   - Key observations on the status of risk management activities in the quarter, including any new risks identified and action taken w.r.t these risks;
   - Status of effectiveness of implementation of the mitigation plan for key risks

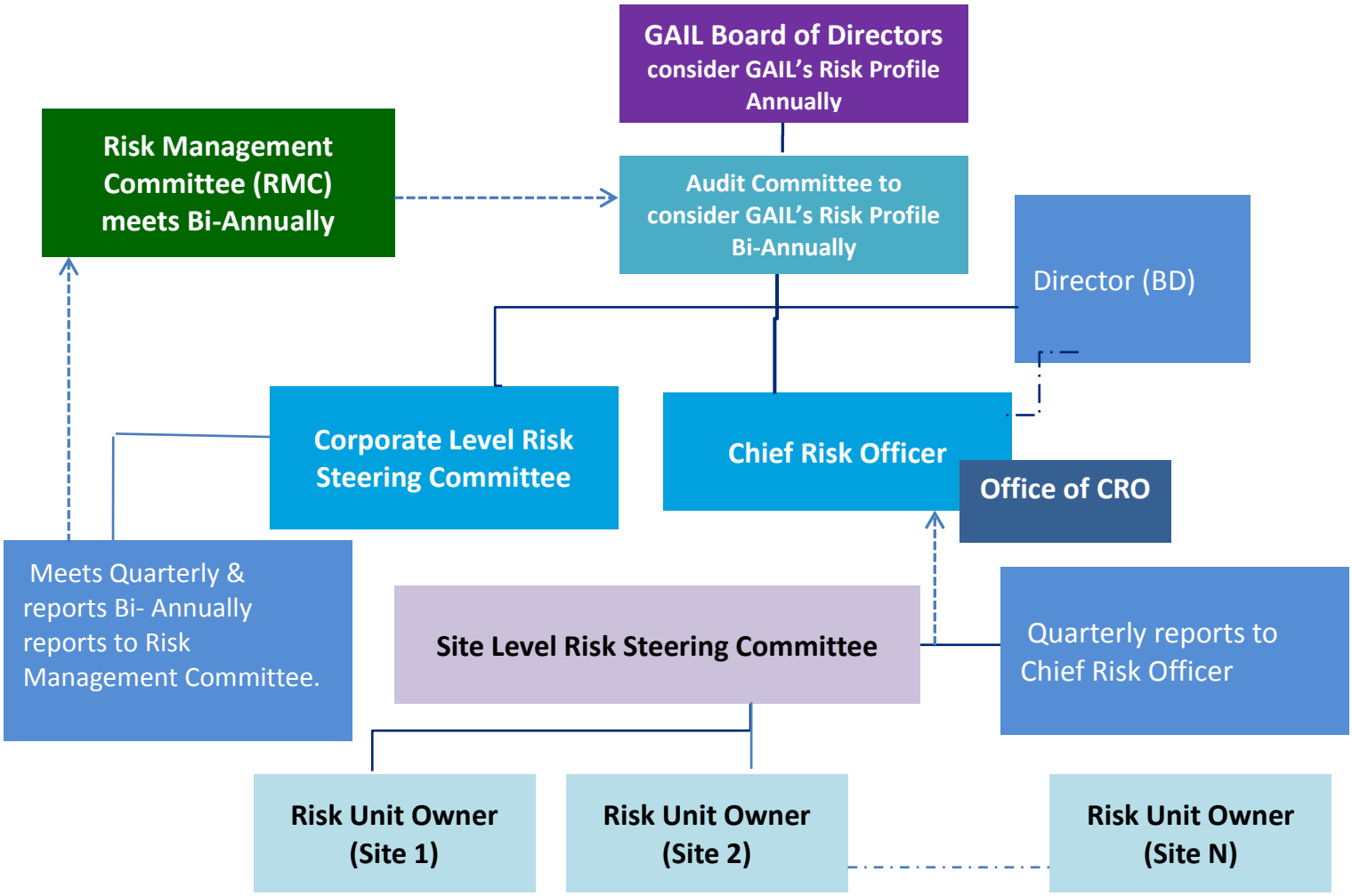
[Refer Appendix II for all the reporting formats]

5.0RISK MANAGEMENT ORGANIZATION STRUCTURE



* As per the existing system, CRO will an officer of the rank of ED / GM along with 4 numbers of cross functional team members will form part of CRO office. Adequate training & exposure will be imparted to the CRO & his team.

Flow Chart for reporting, monitoring and reviewing:



Note: Office of CRO will coordinate all activities.

5.1 Roles and Responsibilities

5.1.1 Board of Directors

The Board, through the Audit Committee shall oversee the establishment and implementation of an adequate system of risk management across the company. Board shall comprehensively review the effectiveness of the company's risk management system on an annual basis.

5.1.2 Audit Committee

The Audit Committee would review on Bi-Annually, the risk assessment & minimization procedures across the Company after review of the same by the Corporate Level Risk Steering Committee. The Audit Committee will assist the Board in independently assessing compliance with risk management practices. It will also act as a forum to discuss and manage key risks.

5.1.3 Risk Management Committee (RMC)

Concerned Functional Director shall review the exception reports along with effectiveness of the mitigation plans sent by the Site Level Risk Steering Committee on Bi-Annual basis. They may advise for inclusion of new risks and modify the mitigation plans.

Functional Directors shall also review the exception reports along with effectiveness of the mitigation plans sent by the Corporate Level Risk Steering Committee on quarterly basis. They may advise for inclusion of new risks and modify the mitigation plans. Effectiveness of the risk management policy & framework shall be reviewed.

5.1.4 Corporate Level Risk Steering Committee

The Corporate Level Risk Steering Committee shall consists of key functional heads of ED/GM level at Corporate Office and one of the functional Director as chairman of the committee. CRO will be the coordinator.

The Committee seeks to identify the key business risks which would prevent the Company from achieving its objectives and ensures that appropriate controls are in place to manage these risks.

Key responsibilities of the Committee include:

- Identification of new risks.
- Monitoring the environment within which the risk exists to identify issues which may affect its impact on the company or the likelihood of its arising
- Providing assurance that risk management policy and strategy of the company are operating effectively
- Developing risk response processes and assessing adequacy of responses for the key risks identified through the risk management framework
- Ensuring the implementation of risk mitigation plans
- Monitoring the Key Risk Indicators (KRIs) of the Enterprise and Functional Level Key Risks.
- Monitoring the performance of different segments
- Preparation and Update of the Corporate Level Key Risk Register and Quarterly reports for the Board/Audit Committee.
- Present the quarterly risk management update report based on the inputs by the CRO Office to the Audit Committee & Functional Directors.

5.1.5 Chief Risk Officer and the Office of CRO

The Chief Risk Officer (CRO) plays a pivotal role in the oversight and execution of a company's risk management function. Working closely with the Director (BD), CMD, Audit committee and the Board, the CRO is responsible for developing and implementing risk assessment policies, monitoring strategies, and implementing risk management capabilities. The CRO's ultimate objective is to help the Board and executive management to determine the risk-reward tradeoffs in the business and bring unfettered transparency into the risk profile of the business. The CRO will be supported by a team of risk analysts, will be known as the Office of CRO or the Risk Office. The CRO office works closely with the business units to identify risks and then evaluate and negotiate risk response plans based on cost-benefit analysis.

As the ERM champion, the CRO facilitates the execution of risk management processes and infrastructure as a key enabler to achieving the business objectives of the organization. Following are the key responsibilities of the CRO and CRO Office:

- Identification of new risks.
- Assist the board and senior management to establish and communicate the organization's ERM objectives and direction;
- Assist management with integrating risk management with the strategy development process;
- Assist the Board and the executive committee to develop and communicate risk management policies.
- CRO will be the Coordinator of the Corporate Level Risk Steering Committee
- Facilitate enterprise-wide risk assessments, developing risk mitigation strategies where required, and monitoring key risks across the organization
- Monitoring the Key Risk Indicators (KRIs) of the Enterprise and Functional Level Key Risks on a continuous basis.
- Assists in establishing, communicating and facilitates the use of appropriate ERM methodologies, tools and techniques
- Works with business units to establish, maintain, and continuously improve risk management capabilities
- Implements appropriate risk reporting to the Board and senior management
- Enables effective alignment between the risk management process and internal audit
- Office of CRO will be responsible for coordinating with respective risk unit owners and consolidating the quarterly and annual risk register and database review reports.
- Based on the inputs from site/units, the CRO will present the quarterly risk management report to the Corporate Level Risk Steering Committee.

The CRO will be an officer at a level of Executive Director or GM and shall be reporting to the Director (BD). Adequate training & exposure will be imparted to the CRO & his team.

5.1.6 Site Level Risk Committee

The Committee will set the risk management procedures and coordinate with risk unit owners in reporting key risks to the Corporate Level Risk Steering Committee by following the standard operating procedure. Key responsibilities of the Committee include:

- Identification of new risks
- Performing the review of the Risk Register on quarterly and Risk Database annually.
- Review reports prepared by the individual risk unit owners.
- Assisting the various risk units to identify, analyze and manage risks
- Developing risk response processes
- Monitoring the Key Risk Indicators for key risks at the site level on a continuous basis
- Identifying the areas, which need insurance or financial cover to protect against loss
- Ensuring the implementation of risk mitigation plans
- Escalation of issues requiring policy approvals and amendments to the Corporate Level Risk Steering Committee and CRO.

- OIC/ HOD at Corporate office will be the chairman of the site level risk steering committee.

5.1.7 Risk Unit Owner

Risk unit owners in consultation with OIC at a plant/unit will assess the risk by determining its probability of occurrence and its impact with an objective of reporting key risks to the Site Level Risk Steering Committee.

Key responsibilities of the Risk unit owners include:

- Identification of new risks
- Reviewing and discussing significant risk issues and ensuring horizontal collaboration in the development of mitigation strategies and the establishment of corporate priorities in resource allocation
- Reporting new risks or failures of existing control measures with remedial action to Site Level Risk Steering Committee.
- Keeping the risk registers and related action plans updated
- Consolidating the quarterly and annual risk register and database review reports and timely reporting to the Office of CRO
- Submission of the quarterly risk register review report by the 10th day following the quarter end to the office of CRO.
- Submission of the annual risk database review report by the 45th day after the financial year end, to the office of CRO.
- Educating employees dealing with key activities in their unit of the risk management process
- Facilitating segment level and corporate level steering committee meetings
- Ensuring Management Action Plans developed in response to audit and evaluation recommendations adequately address the risks identified
- Providing management with information about the organization's controls and determining which controls should be in place to adequately lower the overall risk profile of various critical processes

5.1.8 Risk Unit Officer

Risk unit officer assists Risk Unit Owner in carrying out the secretarial work. Risk unit officer is designated by the Risk Unit Owner.

5.1.8 Internal Audit

Key responsibilities of Internal Audit Group related to risk management shall include:

- Implement a risk-based approach to planning and executing the internal audit process.
- Internal audit resources to be directed at those areas which are key and/or significant as brought out periodically through the risk management process.

5.2 Risk Management Activity Calendar

Activity	Timelines
Risk Register Review report to be submitted by risk unit owners to the CRO	Quarterly By 10th day following the quarter end
Risk Database review report to be submitted by risk unit owners	Annual By 45th day following the financial year end
Corporate Level Risk Steering Committee meeting to review the Corporate key risks/ reports from site/ units	Quarterly
Review by Risk Management Committee	Bi-Annually
Audit Committee meeting	Bi-Annually
Board meeting	Annually

APPENDIX

APPENDIX I

RISK RATING CRITERIA

The Risk Rating Criteria, a key element of the risk management framework seeks to establish the standard for prioritizing the risk based on the assessment of the following:

• **Impact** of the risk on the stated objectives and goals: The degree of consequences to the organization should the event occur

• **Likelihood** of occurrence of the risk: The likelihood of the event occurring expressed as an indicative annual frequency

IMPACT CRITERIA DEFINITIONS

	Consequence Descriptions					
Impact	**Profit Reduction/ Loss in % per year**	**Health and Safety**	**Natural Environment**	**Social or Cultural Heritage**	**Community, Government, Reputation, Media**	**Legal**
1 - Negligible		No medical treatment required	Minor effects on biological or physical environment	Minor, medium-term social impacts on local population; mostly repairable	Minor, adverse local public and media attention	Minor legal issues
2 - Minor	< 1 %	Objective but reversible disability requiring hospitalization	Moderate, short-term effects but not affecting ecosystem functions	Ongoing social issues; permanent damage to items of cultural significance	Attention from media; heightened concern by local community	Noncompliance and breaches of regulation
3 - Moderate	1 % - 5 %	Moderate irreversible disability or impairment to one or more persons	Serious medium-term environmental effects	Ongoing serious social issues; significant damage to structures or items of cultural significance	Criticism by national government	Serious breach of regulation with investigation or report to authority with prosecution or moderate fine possible
4 – Major	5 % - 15 %	Single fatality or severe, irreversible disability to one or more persons	Very serious, long-term environmental impairment of ecosystem functions		Significant adverse national media or public or national government attention	Major breach of regulation; major litigation
5 - Severe	> 15 % or #	Multiple fatalities or significant, irreversible effects to >50 persons			Serious public or media outcry; international coverage	Significant prosecution and fines; very serious litigation including class actions

if the profit reduction/ loss is more than Rs. 100 Crore per year, impact will be considered as severe (i.e scale 5)

LIKELIHOOD CRITERIA DEFINITIONS

	Probability Descriptions		
Likelihood	**Occurrence in future**	**% Chance**	**Occurrence in past**
1 – Rare	Not likely, almost impossible to occur between two (from now) to five years.	Less than 5%	Similar instances have never occurred in the past.
2 – Not Likely	May occur once or twice between two (from now) to five years.	5 to 9%	Though not routinely but there have been instances in the last 2 to 5 years.
3 – Likely	Possible, may arise once or twice within the next year.	10 to 49%	There have been one or two similar instances in the past year
4 – Highly Likely	High, may arise several times within the next year.	50 to 80%	Similar instances have occurred several times in the past year
5 – Expected	Very high, will be almost a routine feature every month within the immediate next year.	Over 80%	Similar instances have commonly occurred every year in the past.

LIKELIHOOD CRITERIA DEFINITIONS – SCORING MAP

	Impact				
Likelihood	**1 - Very Low**	**2 – Low**	**3 – Moderate**	**4 - High**	**5 - Very High**
1 – Rare	Low	Low	Low	Low	Low
2 – Not Likely	Low	Low	Low	Medium	Medium
3 – Likely	Low	Low	Medium	High	High
4 – Highly Likely	Low	Medium	High	High	High
5 - Expected	Low	Medium	High	High	High

RISK RATING

Level of Risk	Description	Rating (Impact * Likelihood)
HIGH	High risk. Senior management attention needed to develop and initiate mitigation plans in the near future	**> 12**
MEDIUM	Moderate Risk. Functional Heads attention required	**Between 8 to 12**
LOW	Low Risk. Manage by routine procedures	**< 8**

APPENDIX II

REPORTING FORMATS AND TEMPLATES

A. Quarterly Risk Register Review Report

Quarterly Risk Register Review Report **Unit <To be updated>**							
Function	**Risk Description**	**Risk Register Reference**	**Trigger Events**	**Risk Score**	**Proposed Risk Mitigation Plan**	**Status of implementation of Risk Mitigation Plan**	**Action Plan based on KRIs**
Risk Unit Owner: <Name>							
(Signature)		(Designation)			(Date of approval)		
Site Risk Committee Meeting held on:							
Chairman of the Site Level Risk Steering Committee: <Name>							
(Signature)		(Designation)			(Date of approval)		
Comments:							
Approved by Site OIC: <Name>							
(Signature)		(Designation)			(Date of approval)		
Comments:							
Presented to the Office of Chief Risk Officer							

B. Annual Risk Database Review Report

Annual Risk Database Review Report **Business Unit : <…….>**							
Function	**Risk Description**	**Risk Database Reference**	**Risk Score**	**Proposed Risk Mitigation Plan**	**Status of implementation of Risk Mitigation Plan**	**Changes to risk ratings or risk scenario**	**Additional Comments**
Risk Unit Owner: <Name>							
(Signature)			(Designation)			(Date of approval)	
Site Risk Committee Meeting held on:							
Chairman of the Site Level Risk Steering Committee: <Name>							
(Signature)			(Designation)			(Date of approval)	
Comments:							
Approved by Site OIC: <Name>							
(Signature)			(Designation)			(Date of approval)	
Comments:							
Presented to the Office of Chief Risk Officer							

C. Risk Movement Report

To be filled up by the risk unit owner and submitted to the Office of CRO in case there are any changes in the risk ratings

Risk Movement Report							
Risk Movement		**Risk Description**	**Risk Register Reference**	**Movement Caused by change in**		**Reasons for change**	**Proposed Risk Mitigation Plan**
From	**To**			**Impact**	**Likelihood**		
Risk Unit Owner: <Name>							
(Signature)			(Designation)			(Date of approval)	
Site Risk Committee Meeting held on:							
Chairman of the Site Level Risk Steering Committee: <Name>							
(Signature)			(Designation)			(Date of approval)	
Comments:							
Approved by Site OIC: <Name>							
(Signature)			(Designation)			(Date of approval)	
Comments:							
Presented to the Office of Chief Risk Officer							

D. Quarterly Key Risk Report

Presented to the Corporate Level Risk Steering Committee by the Chief Risk Officer

Quarterly Key Risk Report							
Quarter Ending: <--------->							
Function	**Risk Description**	**Risk Category**	**Risk Score**	**Proposed Risk Mitigation Plan**	**Status of implementation of Risk Mitigation Plan**	**Changes to risk ratings or risk scenario**	**Action Plan based on the KRIs monitoring**
Number of Key Risks as per the previous review:							
Number of Key Risks as per the current review:							
Chief Risk Officer							
(Name)			(Designation)			(Signature)	
Comments:							
Presented to the Corporate Risk Management Steering Committee							
Corporate Level Risk Steering Committee Meeting held on:							