RISK MANAGEMENT POLICY

NACL Industries Limited

DOCUMENT CONTROL

RISK MANAGEMENT POLICY AND PROCEDURES for NACL Industries Limited	
Version 1.0	
Authorized By: Risk Management Committee	Date: December 15, 2025

RISK MANAGEMENT POLICY Version 1.0

For Restricted Circulation

FOREWORD

The pursuit of opportunity in any human endeavor means leaving the status quo, the safe haven-the tried and true. General MacArthur once said "***There is no security on this earth. Only opportunity.***" The statement explicitly implies that security is nonexistent. Efforts to achieve security by standing still, hunkering down or attempting only that which has been attempted in the past will not produce security. Indeed, such actions will generate risks on their own. Yet, as we all know, risks also accompany the pursuit of opportunity.

Managing the risks that accompany the pursuit of opportunity – or, more precisely, the pursuit of value – is the main of objective of Enterprise Risk Management (ERM). Executives who are mainly accustomed to risk avoidance often fail to identify, appreciate and manage risks that attend the pursuit of value. This occurred across a range of industries, and it is chiefly because of conventional approaches to risk management.

Executives make important decisions, often without complete information in a complex changing environment characterized by uncertainty and turbulence. "Risk Intelligence" is an approach to conducting business that improves decision making and judgment in vital areas and initiatives. Risk Intelligence is dynamic. It is a process that needs to be followed continuously to create value and manage risks that enable better decisions.

Conventional risk management separates risks from strategic and operational decisions and tends to view it in isolation. It makes ERM episodic, isolated in silos, specialized and therefore lacks integration across enterprise, strategy, execution and operation. Risk Intelligence on the other hand generates awareness of risks at all levels within an integrated framework to obtain best intelligence available with the view to achieve decision superiority and competitive success.

NACL's Enterprise Risk Management framework is designed to create a robust and integrated approach which details with the strategic and operational process of the organization. The process will involve the steps delineated below:

- Checking Assumptions
- Maintaining Constant Vigilance
- Factoring in Velocity and Momentum
- Managing the Key Connections
- Anticipating the Causes of Failure by identifying triggers and causal factors
- Verifying Sources and Corroborate Information
- Maintaining Safety Targets by understanding the consequences and measuring the impact
- Setting Time Horizons
- Taking the Right Risk
- Sustaining Operational Discipline

This will help generate a rationalized approach to identifying, discussing, measuring and managing vital opportunities and risks the enterprise faces. The framework will enable the operating leaders, across the organization, to be aware of the process to ingrain risk management into the DNA of every employee of the organization, with a view to enhance enterprise value.

STRATEGIC OBJECTIVES

Conventional risk management separate risks from most strategic decisions and tends to view it in isolation. It also concerns itself mainly on potential financial risks and tends to ignore risks relating to brand, people, reputation, operations etc. Conventional risk management tends to be episodic, specialized, isolated in silos, and lacking integration across the enterprise and across strategy, execution, and operations.

Unconventional risk management understands the triggers and causal factors affecting the risk event with the objective of establishing a structured and intelligent approach towards identifying the key risk indicators. In other words, it focuses first on the causes of the risks rather than the risk per se. On the other hand, it links the KRIs with the consequences and impact to comprehend the risk effect. This approach provides a cause-effect analysis of the risks and maps it across the organization. The cause and effect are mapped on two axes, i.e. the likelihood factor and the risk quotient to understand the full impact of the risk against the entities, risk appetite and risk capacity. This approach will enable NACL to create a "Risk Intelligent" organization. The process begins by articulating the Vision and Mission statements and delineating the Strategic Objectives. The vision and mission statements of NACL's relative to ERM are:

Vision

NACL will be "Risk Intelligent" organization by integrating the ERM initiative into strategic and operational decision-making processes. The Board, the executive management and the business functions will ensure the optimal balance of risk and reward whilst pursuing their strategic and business objectives.

Mission

- Create an organization culture and an organization structure where risks are looked as opportunities to create value and prevent value depletion.
- Create an organization environment where risk is considered as everyone's responsibility
- Encourage employees to call out on risk indicators and bring out weaknesses in risk response plans on an ongoing basis
- Encourage continuous improvement in the ERM process

Strategic Objectives

The ERM program's mission, vision, and strategic directions translate into the strategic objectives which are shown below. This section also describes how these ERM objectives support the Company's strategy and the necessary supporting infrastructure.

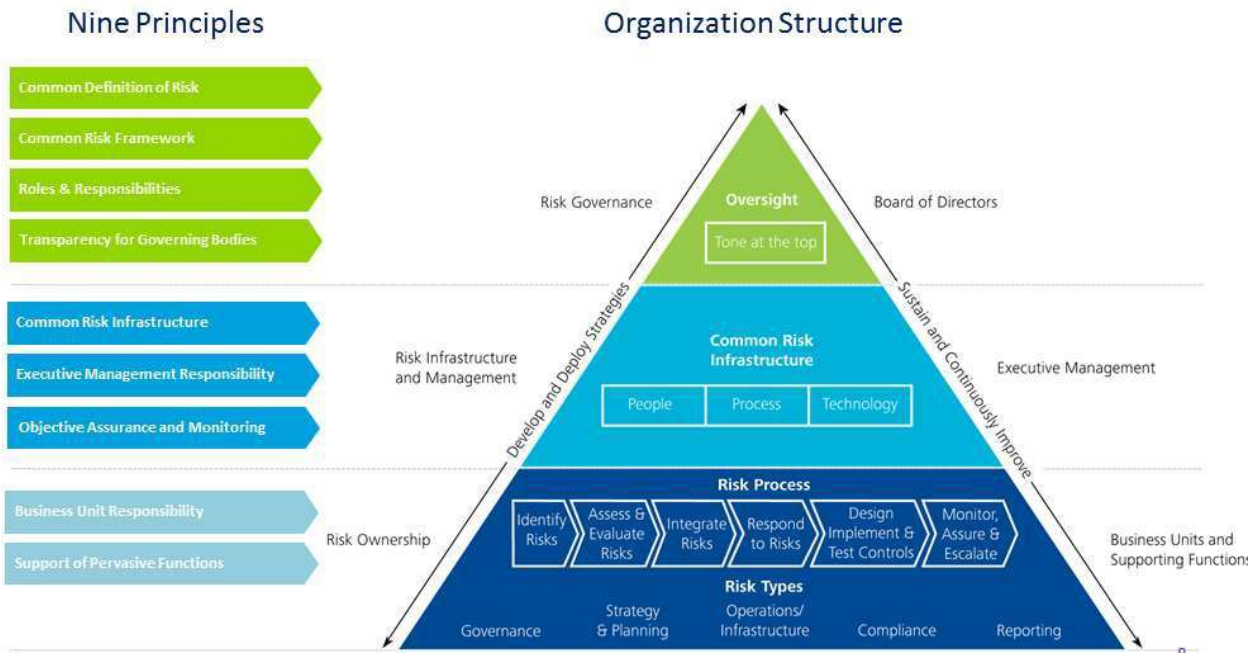
- Launch an ERM eminence building program
- Integrate enterprise risk management into daily activities of the NACL across all business units
- Ensure the optimal balance of risk and reward whilst pursuing its objectives
- Promote a risk management culture where risk is everyone's business from the Board room to the field and plant
- Recruit, develop, and deploy leading ERM practitioners
- Implement risk management best practices in all activities related to its businesses
- Link strategic decision-making process with risk management in all its business areas and maximize their integration
- Aggregate and manage risks as a portfolio

The following table lays down the alignment of ERM's strategic objectives with the Company's business Strategies

Strategic Dimensions	**Business Strategies**	**Strategic Statements**
Financial	Profitability	Ensure the optimal balance of risk and reward whilst pursuing top and bottom-line growth.
Regulatory	Compliance	Adherence to laws, regulations, guidelines and specifications relevant to Company's business.
Stakeholder/Peer/Customer	Secure and sustain reliable business partners	Implement risk management best practices in all business partner management activities related to the businesses of the Company.
Internal Business Processes	Operational Excellence E.g.: a) Sourcing of raw material /intermediates/finished goods	Integrate enterprise risk management into the Company's daily activities/operations and those of its business units.
	Manage Risks	Aggregate and manage risk as a portfolio and take a holistic view of risks.
	Best in Class Safety, Health & Environment (SHE)	Implement risk management best SHE practices in all activities related to its businesses.
Learning and Growth	Effective Communication	Promote a risk management culture where risk is everyone's business from the Board room to the field and plant.
	Employer of Choice	Recruit, develop, and deploy leading ERM practitioners.
	Technology	Implement in the medium term an IT enabled Risk management solution that integrates activities related to the business.

1.1 ERM INFRASTRUCTURE

To support the above objectives, it is imperative that the NACL has a robust ERM infrastructure (the nine principles) built on the principles of good Governance, People centric environment, well defined Processes and enabling Technology. The organization structure should lend itself to this infrastructure to make it robust. The dovetailing of the two is depicted below:

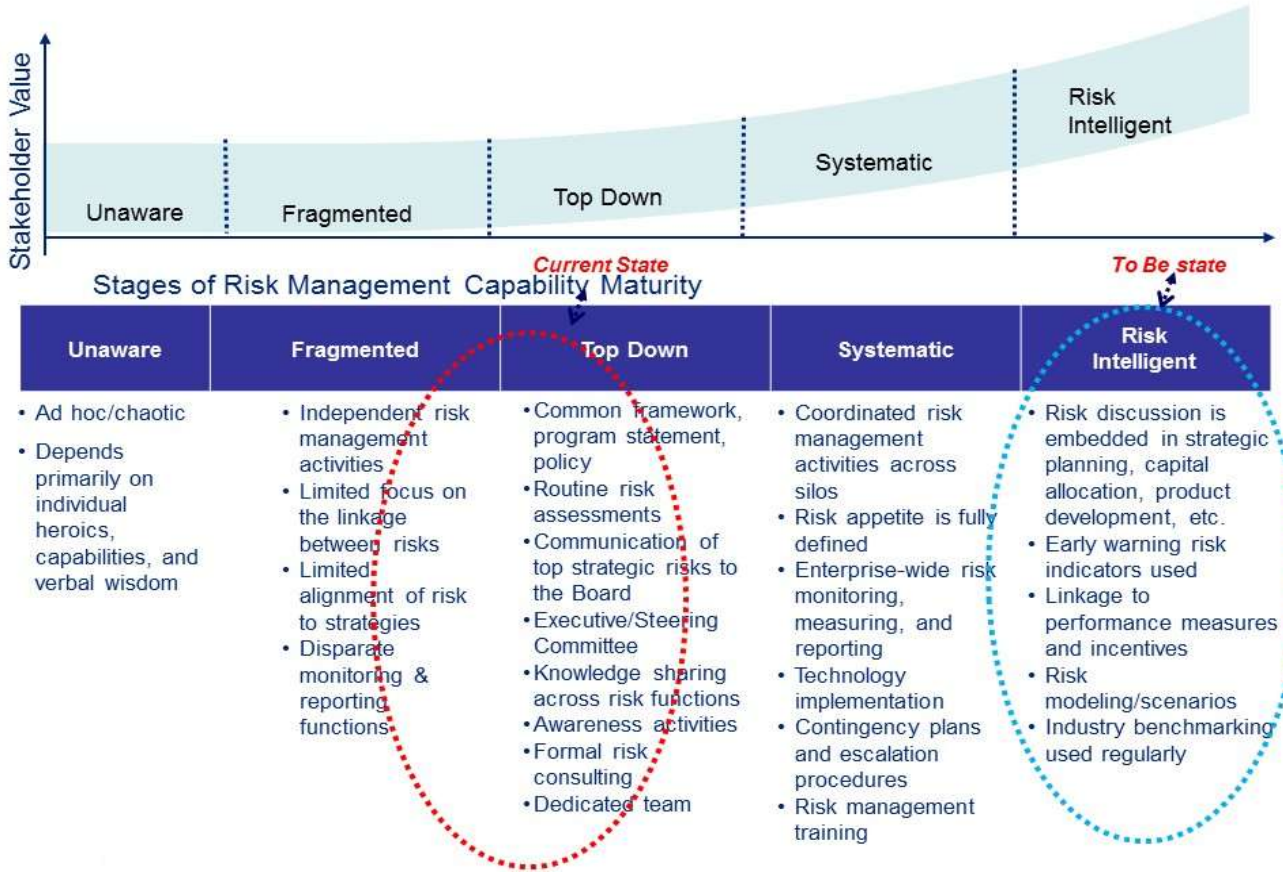


The above synchronization is of seminal importance because it generates awareness of risks at all levels within an integrated framework/infrastructure to obtain best intelligence available under the circumstances. This makes the NACL "Risk Intelligent" and thus the goal to achieve decision superiority and competitive success is fulfilled.

2.0 METHODOLOGY

2.1 THE RISK MANAGEMENT FRAMEWORK

- NACL has a supporting infrastructure necessary to establish its ERM program at the Comprehensive maturity level (depicted in below picture) with some gaps to fill. To achieve its ERM strategic objectives, NACL has now implemented additional supporting infrastructure elements. This will result in movement along the Capability Maturity continuum from Comprehensive to Integrated to Strategic levels in its ERM ecology. Given below is NACL's Comprehensive maturity level



- To make the shift from the "Comprehensive" state to an "Integrated" environment it is important to have a comprehensive Enterprise Risk Management (ERM) framework. NACL's ERM framework covers the full-spectrum approach to risk management that includes identifying, assessing, measuring, monitoring, and responding to risks across the enterprise. When properly executed, ERM activities are aligned with strategic objectives and are conducted within the limits of a predefined risk appetite. ERM addresses a framework for identification of Internal & External risks specifically faced by the company in particular:

  - ✓ Strategic.
  - ✓ Financial.
  - ✓ Operational.

- ✓ Sectorial.
- ✓ Sustainability matters (Environment, Society & Governance – ESG);
- ✓ Information.
- ✓ Cyber Security risks.
- ✓ Compliances & Safety; and
- ✓ Any other Risks as determined by the Committee

- ERM ensures that NACL and its stakeholders are protected and value creation is carried out by improving the decision-making processes, proactively planning and prioritizing the risks by comprehensive and structured understanding of the activities carried out by the enterprise, the volatilities and threats it is exposed to and how to convert such threats into opportunities.

  The risk framework would enable the NACL to carry out ERM activities in a consistent and controlled manner. The framework will also help to create an environment where risk management is practiced consistently across the NACL with the management taking informed decisions that would reduce the possibility of surprises.

- The components that would define risk management would be dependent on the NACL's business model, its strategies, organizational structure, organization culture, its appetite for risk and a team of dedicated resources to address the risks. NACL's risk management framework consists of a set of consistent processes that can assess, mitigate, monitor and communicate any risk related issues across the organization. Thus, aligning the risk management process with the corporate direction and objectives, specifically strategic planning and annual business planning processes becomes essential. Risk management is a continuous and evolving endeavor, which will always be ingrained within the culture of the NACL.

  The Risk Management Framework of the NACL comprises:

  - Risk Management Policy which lays down the structure of the process at entity and business levels
  - Risk Management Organization structure which facilitates the implementation of the policy thereby enabling effective functioning of the enterprise-wide risk management process

- Risk Management process comprises 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.

- The risk management framework adopted by NACL is mapped as to the ISO Standard 31000:2018 Risk Management - Principles and guidelines and is also in-line with recommendations of The Committee of Sponsoring Organizations of the Treadway Commission ("COSO"). The enterprise-wide comprehensive risk management view/ framework will help address both inherent and residual risks emanating from internal and external factors such as operations, strategy, finance regulatory, macro-economic changes etc. and their consequent impact on the organization. Given below is a comparative representation of ISO 31000:2018 process for managing risks and the Company's ERM framework.

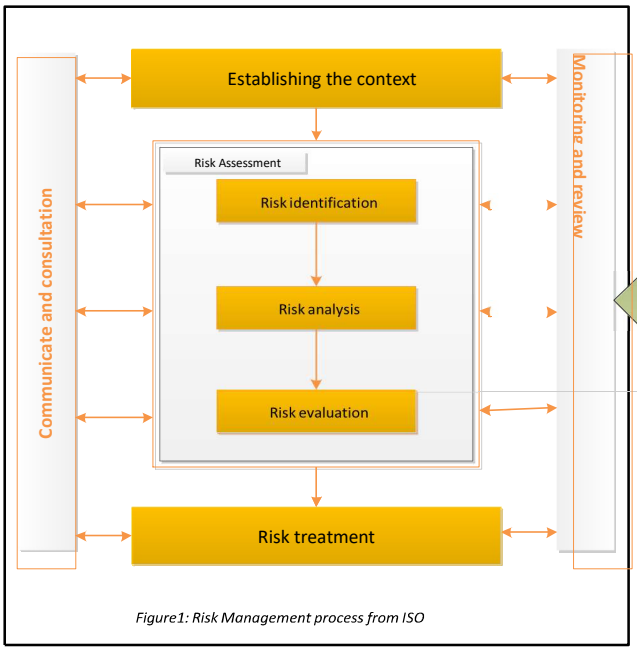


Figure1: Risk Management process from ISO

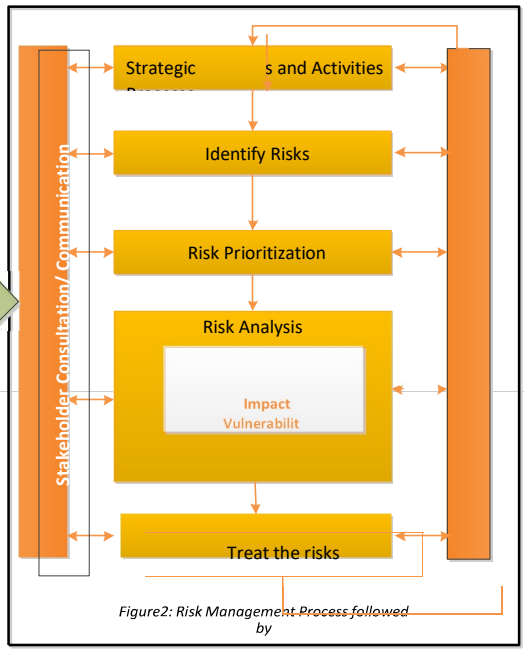


Figure2: Risk Management Process followed by

- The risk management framework is also aligned with the COSO framework. It defines essential components, suggests a common language, and provides clear direction and guidance for ERM. Entity objectives can be viewed in the context of four categories of Strategic, Operations, Reporting and Compliance also ERM considers activities at all levels of the organization Viz. Enterprise level, Business Unit, Functional and Operations. Given below is a comparative representation of COSO framework and the Company's ERM framework

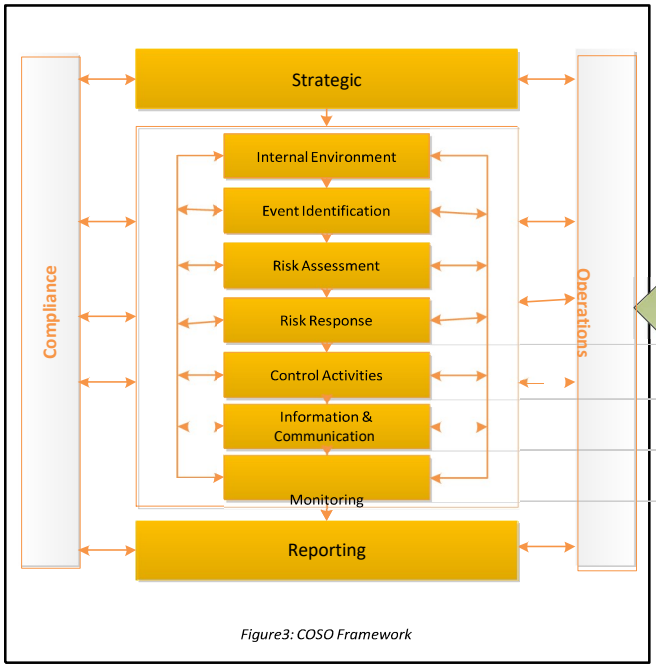


Figure3: COSO Framework

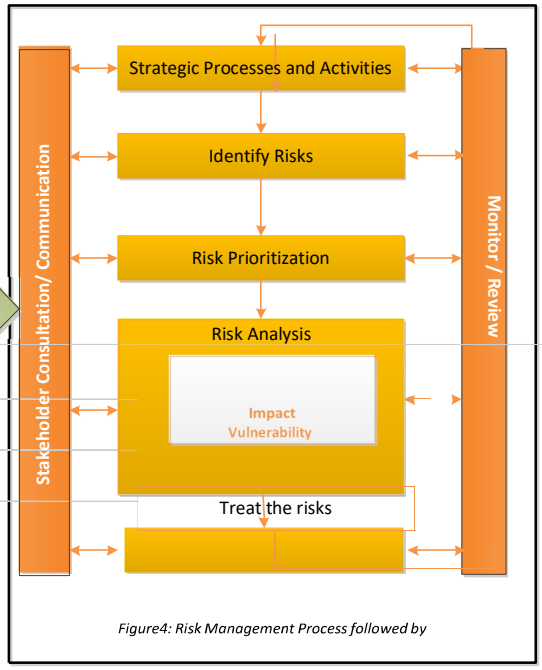


Figure4: Risk Management Process followed by

2.2 RISK MANAGEMENT STRUCTURE

The risk management process is supported by a risk management structure primarily comprising of:

- Governance
- Risk organization structure
- Roles and Responsibilities
- Risk management activity calendar

2.2.1 Governance & Risk Management Organization Structure

In this section we present several key elements of the risk governance structure for NACL to consider in enhancing its ERM program. We start with the broad question of how centralized or decentralized NACL's ERM program should be. We then address each key organizational unit from the Board of Directors to the ERM function.

There are four important forms of oversight that are included in the organizational structure in order to provide appropriate checks and balances. These forms of oversight are listed below and are reflected in the proposed risk governance structures throughout this section:

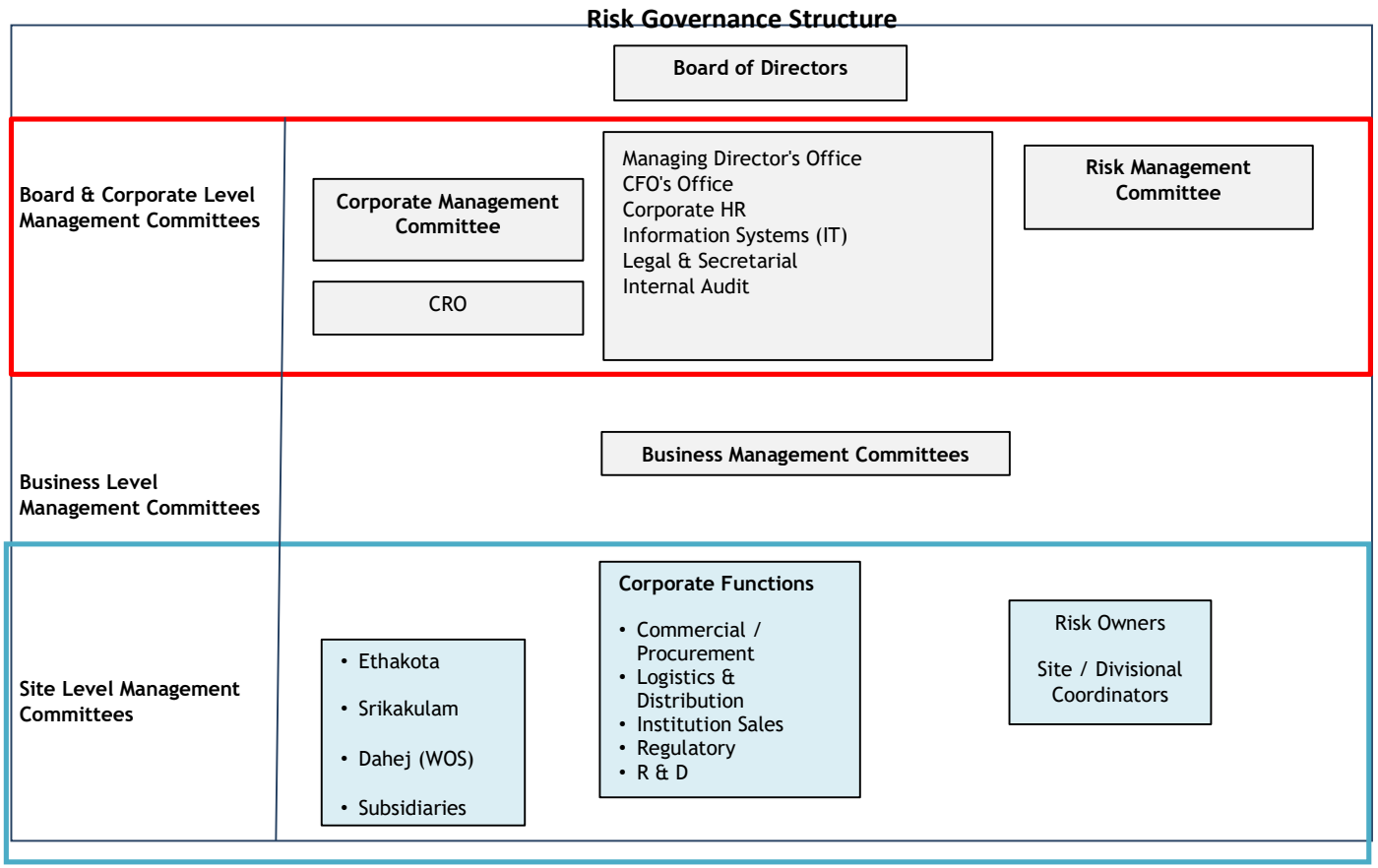
1. Oversight by the Board of Directors.
2. Oversight by the Chief Risk Officer and Risk Management Committee (RMC) of NACL.
3. Direct supervision by Corporate Management Committee (CMC), Business Unit Management Committee (BMC) and Site Level Risk Management Committee (SLMC).
4. Independent risk management, compliance and audit functions. Internal audit would provide assurance to the Board that the risk management processes being undertaken are in direct support of corporate objectives.

2.2.1.1 Organization Structure

The Risk Management Policy is implemented through the establishment of a Risk Organization Structure. At the core, is the office of Chief Risk Office headed by the Chief Risk Officer (CRO). Chief Risk Officer will be of the position of Vice-President / General Manager.

2.2.1.2 Risk governance structure

The diagram below depicts the relationship between the key risk governance elements. The Head internal Audit should not participate in management decisions regarding risk taking in order to preserve his/her independence unless he/she is also the CRO. Internal Audit's independent role is crucial to the organization.



Hybrid Model

NACL follows hybrid model in which the business units/and managerial divisions/functions assume primary responsibility for identifying, prioritizing, quantifying risks and reporting on Key Risk Indicators (KRIs). The centralized Risk Management Department carries out the functions - consolidate information about the highest priority key group risks for the Risk Management Committee and facilitates analysis of cross-business divisions risks. The Risk Management Committee also analyses risk mitigation decisions about the key group risks. The business units retain authority to make risk mitigation decisions about risks that reside within their business units.

2.2.2 Roles & Responsibilities

2.2.2.1 Board of Directors

The Board has delegated detailed risk analysis to the Risk Management Committee given their level of interest and specialization. The Board, through the Risk Management Committee, is responsible for overseeing the establishment and implementation of an adequate system of risk management across the company. The Committee is responsible for comprehensively reviewing the effectiveness of the Company's risk management process on an ongoing basis. The Committee approves the risk appetite statement (defined in section 2.3.2.7); accept accountability for authorizing NACL's risk appetite and tolerance thresholds, for performing risk oversight, and for integrating risk oversight with strategic decision making.

The Board will, however, retain risk oversight at the full Board to incorporate consideration of risk into strategic decision-making and to address risk interactions across various businesses. It will review at least once a year the effectiveness of ERM process, the risk universe and the robustness of the risk response plan.

2.2.2.2 Risk Management Committee

The Risk Management Committee (RMC) shall comprise one of the members of the Board of Director as chairman of the committee and other members as nominated by the Board of Directors / chairman. RMC invites the following individuals to the committee meeting as per the requirements, invitees consist Chief Financial Officer, Chief Risk officer, key functional heads of the Manufacturing, Marketing, Information Technology, Finance & Treasury, Safety, Health & Environment, Public Relations & Communications, Human Resources, Business units, Head of Internal Audit at Corporate Office and any other person invited by the committee. RMC will review the effectiveness of the ERM process across the Company. The Committee will assist the board in independently assessing compliance with risk management practices. It will also act as a forum to discuss and manage strategic and key operational risks.

RMC is also responsible for reviewing the enterprise level key risk register with focus on critical risks with specific containment or elimination plans. RMC will review the risk management policies and the ERM process once in 2 years and receives half yearly update from the CRO. In addition to bi-annual review, the policy may be reviewed by the committee at more frequent intervals if the situation warrants. The RMC conducts half yearly meetings or as and when circumstance arises or as decided by the board.

The Committee will deliberate on the new key risks presented by the CRO and act as a sounding board to the CRO.

Key responsibilities of the Committee to help and advise the office of the CRO in

- Ensuring that the functions are providing enough support in proper functioning of ERM
- Helping in effective implementation of the ERM program
- Discussing the impact and mitigation plan of all key risks through the risk management framework
- Ensuring that mitigation plans are implemented effectively and timely.

- Providing support and guidance in implementing risk based strategic decisions
- Apprising the Board, on the effectiveness of risk management policies, ERM Processes and activities of RMC

2.2.2.3 Chief Risk Officer and the Office of CRO

The Chief Risk Officer (CRO) plays a pivotal role in the management and execution of a Company's risk management function. Working closely with the Risk Management Committee, the CRO is responsible for developing and implementing risk assessment policies, monitoring strategies, implementing risk management capabilities, reporting and monitoring. The CRO's ultimate objective is to help the Board and executive management to determine the risk-reward tradeoffs in the business/function and bring unfettered transparency into the risk profile of the business. The CRO will be supported by a team, the CRO's office will work closely with the business units to identify risks and then evaluate and execute risk response plans based on cost-benefit analysis. The CRO will participate in Corporate Management committee, Business unit Management committee and Site level Management committee meetings.

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. However, CRO is **not the owner** of the risks of the entity. The risks are owned by the respective Risk owners. Following are the key responsibilities of the CRO and CRO Office:

- Establish and communicate the organization's ERM objectives and direction.
- Integrate risk management with the strategic decision-making process.
- Coordinate with the Risk Management Committee chairman and members
- Provide an independent view regarding new investment proposals and projects, including validation of risks, if any.
- Facilitate enterprise-wide risk assessments, developing risk mitigation strategies where required, and monitoring High risks across the organization
- Determine the risk appetite of the enterprise (defined in section 2.3.2.7).
- Monitor the Key Risk Indicators (KRIs) of the Enterprise, Business unit level and Functional Level High Risks on a continuous basis.
- Implement ERM methodologies, tools and techniques
- Work with business units to establish, maintain, and continuously improve risk management capabilities
- Implement appropriate risk reporting mechanisms
- Enable effective alignment between the risk management process and internal audit

- Policy revision requests received from site and business unit committees will be presented to Corporate Management Committee. All changes made to policy should be approved by the Risk Management Committee

Office of CRO will be responsible for coordinating with respective Chairman of CMC, BMC and SLMC for consolidating the monthly, quarterly, and annual risk register and database review reports.

Based on the inputs received from respective committees, the CRO will prepare a cumulatively consolidated half yearly report for risk management committee.

The CRO should be an experienced senior officer of the Company who has holistic view of all business/functional aspects of the Company and good understanding of the industry and the world economy. He should possess good analytical & people skills and should have gravitas to interact with the Board. CRO will report functionally to the Risk Management Committee and administratively to Managing Director & CEO. Also, CRO should maintain a close relationship with the CFO and the Head of Internal Audit of the Company.

2.2.2.4 Corporate Management Committee

The Corporate CMC shall comprise of Managing Director, Chief Financial Officer, Chief Risk Officer, Presidents, Senior Vice President/Vice Presidents and other Key functional and business heads. **Managing Director** will be the Chairperson of the Committee.

Key responsibilities of the committee include:

- Performing the review of the business unit Risk Register on quarterly and Risk Database annually or event based
- Review the effectiveness of mitigation / risk response plants prepared by the Business units.
- Assisting the various business units to identify, analyze and manage risks
- Monitoring the Key Risk Indicators for high risks and risk velocity at the entity level on a continuous basis
- Escalation of issues requiring policy approvals and amendments to the Risk Management Committee and CRO.

The Committee meetings to be conducted on a half yearly basis. The CRO will act as a coordinator for the meetings on risk related issues.

2.2.2.5 Business Unit Management Committee

Significant increase in the size of business of requires to create sub-functional risk committees to enhance the effectiveness of Risk Management. Manufacturing Risk Committee:

Manufacturing Head would be the Chairman of the Committee. Unit Heads & Key functional & Department Heads, including Procurement Head, would be members of the Committee.

Marketing Risk Committee:

Marketing Head would be the Chairman of the Committee and Key functional & Department Heads would be members of the Committee.

The meetings are to be conducted on a quarterly basis:

The CRO will act as a coordinator for above Risk Committee meetings.

Key responsibilities of the Committee include:

- Performing the review of the business unit Risk Register and Risk Database on quarterly or event based
- Review the effectiveness of risk response plan reports prepared by the individual risk unit owners at quarterly meetings or event-based meetings at each business unit level
- Assisting the various functions and departments within business units to identify, analyze and manage risks
- Monitoring the Key Risk Indicators for High risks at the SBU level on a continuous basis
- Identifying the areas which need insurance or financial cover to protect against loss
- Reviewing the risk response plans
- Escalation of issues requiring policy approvals and amendments to the Corporate Management Committee and office of CRO.
- Consolidating the quarterly and annual risk register and database review reports and timely reporting to the Office of CRO and respective committees in which he is member of.
- Submission of the quarterly high risk register review report including KRI-KPI report by the 20th day following the quarter end to the office of CRO and respective committees in which he is member of.
- Submission of the annual risk database review report by the 25th day after the financial year end, to the office of CRO and respective committees in which he is member of.

Site Level Management Committee

The Site level Management Committee shall comprise head of the site/plant, key functional heads of the site/plant.

The Committee will set the risk management procedures and coordinate with risk unit owners in reporting High risks to the Business Unit Management Committee by following the standard operating procedure. Key responsibilities of the Committee include:

- Create an environment of continuous self-review
- The process of preempting risk events and just-in-time reporting of new critical events

- Review the level of readiness in responding to risk events
- Stem test risk response plans and report to CRO on its effectiveness
- Encourage risk awareness through various programs, assess the level of awareness and report to CRO
- Take preventive and corrective measures where there are control failures and report to CRO
- Review of robustness of risk response plans
- Review changes in risk velocity
- Assisting the various risk unit owners to identify, analyze and manage risks
- Monitoring the Key Risk Indicators for High risks at the site level on a continuous basis
- Escalation of issues requiring policy approvals and amendments to the Business level Management Committee and office of CRO.
- Educating risk unit owners dealing with key activities in their operation of the risk management process
- Consolidating and reviewing the monthly and annual risk register and annual risk database reports and timely reporting to the Office of CRO and respective committees in which he is member of.
- Submission of the monthly high risk register review report including KRI-KPI report by the 18th day following the quarter end to the office of CRO and respective committees in which he is member of.
- Submission of the annual risk database review report by the 22nd day after the financial year end, to the office of CRO and respective committees in which he is member of.
- Submission of any other reports/information required by the office of CRO and other committees in which he is member of.

Site in charge at plant location will be the chairman of the Site Level Management Committee. His primary role is facilitating site level management committee and participating in Business unit level management committee meetings. The committee meetings are conducted on every month or the event based. For details refer to SLMC charter.

2.2.2.7 Unit Risk Owner

Unit risk owners in consultation with Head of the plant/business unit will identify, assess and report on the Key Risk Indicators based on the methodology described in section [2.3]. He/she will report back to the Site Level Management Committee/ Business Unit Management Committee for consultation and concurrence.

Key responsibilities of the Risk unit owners include:

- Reviewing and discussing significant risk issues including potential 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 Management Committee / Business Unit Management Committee.
- Recording the triggers, causal events, consequences, and impact of the new risks. He will also track the status of the KRIs relating to high risks and risks with high impact and low likelihood.
- Monitor the KRIs against the respective KPIs.
- Keeping the risk registers and related action plans updated
- Consolidating the monthly and annual risk register and database review reports and timely reporting to the Office of CRO and respective committees in which he is member of.
- Submission of the monthly risk register review report by the 15th day following the month end to the site level management committee in which he is member of.
- Submission of the annual risk database review report by the 20th day after the financial year end, to the site level management committee in which he is member of.
- Educating employees dealing with key activities in their department of the risk management process
- Ensuring Management Action Plans developed and implemented 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

2.2.2.8 Internal Audit

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

- Leverage the risk data base and the risk registers for IA planning
- Implement a risk-based approach to planning and execute risk based internal audit process
- Direct Internal audit resources to those areas which are key and/or significant as brought out periodically through the risk management process
- For the high risks, IA reviews the documentation, if any deficiencies are identified, the same is communicated to the respective committee
- Independently test the operating effectiveness of the risk mitigation plan

2.2.3 Risk Management Activity Calendar

The calendar is periodic and or event based.

Activity	**Timelines**
Submission of High-Risk Register review report including KRI-KPI report to the Site Level Management Committee by risk unit owners	Monthly – By 15th day following the month end
Submission of Consolidated High Risk Register review report including KRI-KPI report to the CRO and BMC by Site Level Management Committee	Monthly – By 18th day following the month end
Submission of Risk date base review report to Site Level Management Committee by risk unit owners	Annually – By 20th day following the year end
Submission of Risk date base review report to CRO and BMC by Site Level Management Committee	Annually – By 22nd day following the year end
Submission of Consolidated High Risk Register review report including KRI-KPI report to the CRO and CMC by Business unit Management Committee	Quarterly – By 20th day following the quarter end
Submission of Risk date base review report to CRO and CMC by risk Business unit Management Committee	Annually – By 25th day following the year end
Submission of Consolidated High Risk Register review report including KRI-KPI report to the CRO by Corporate Management Committee	Quarterly – By 25th day following the quarter end
Submission of Enterprise Risk date base review report to CRO by Corporate Management Committee	Annually – By 30th day following the year end
Risk Management committee to review Enterprise key risks/reports from BMC and SLMC	Half yearly
Internal audit department to present the report on ERM implementation to RMC and Board	Half yearly – RMC Annual /Event Based – Board
Presentation by RMC to Board on ERM	Annually

2.3 RISK MANAGEMENT METHODOLOGY

An effective risk management process is one which continuously and consistently assesses its business to identify the risks, develops a mitigation plan, monitors and reports the risk indicators identified across the breadth of the enterprise. A well-defined methodology is thus essential for determining corporate direction and objectives. The risk management framework adopted by NACL is mapped as to the ISO Standard 31000:2018 Risk Management - Principles and guidelines and is in-line with recommendations of The Committee of Sponsoring Organizations of the Treadway Commission ("COSO") (refer to page 10). The enterprise-wide comprehensive risk management view/ framework will help address the risks that are inherent to operations, strategy, finance and compliance and their consequent impact on the organization.

The risk management process adopted by the Company has been aligned with their business processes. At the entity and unit/functional/departmental levels several steps have been incorporated to ensure the following:

2.2.3 Internal Environment

2.2.4 Objective Setting

2.2.5 Event Identification

2.2.6 Risk Assessment and Risk Quantification

2.2.7 Risk Response

2.2.8 Control Activities

2.2.9 Information and Communication

2.2.10 Monitoring

ISO Standard 31000:2018 - "Risk Management – Guidelines".

This ISO Standard is an enhanced version of the older ISO 31000:2009 Standard.

NACL to adopt the Primary changes in the standard which include:

- Review of the principles of risk management, which are the key criteria for its success
- Integration of risk management, starting with the governance of the organization and business performance.
- Analysis & Operations to lead revision of mitigation procedures and controls at each stage of the process.
- Streamlining of the content with greater focus on sustainability aspects of Business.

2.3.1 ESTABLISHING THE CONTEXT

Articulate the objectives to be able to define the external, internal and competitor parameters that must be considered while managing risk, and setting the scope and risk criteria for the remaining processes**.**

Establishing the External Context

The external context needs to be understood as it plays an important role in ensuring that the objectives and concerns of the external stakeholders are considered while developing risk criteria. The external context is based on the organization-wide context but emphasizes on specific details of legal and regulatory requirements, stakeholder perceptions including suppliers and business partners and other aspects of risks specific to the scope of the risk management process.

Establishing the Internal Context

The internal context pertaining to the risk management process aims at aligning the organization's culture, structure, strategy and processes. The internal context in the organization influences the way risks will be managed.

Establishing the Competitor Context

With publicly available information, published reports, conference proceedings, and discussions with subject matter experts for evaluating NACL's competitors and ranking their ERM Maturity.

The external, internal and competitor context can include, but may not be limited to the following:

Governance

- Establishing Board-level risk responsibilities and Risk Committee
- Establishing CRO position and new reporting relationships
- Reposition ERM functions at NACL and at divisions at higher levels of authority
- Creating independence between ERM functions and Internal Audit
- Putting risk in the agenda of the Board on a half year basis and the Senior management team on at least a quarterly basis
- Restructuring NACL Management meetings to focus on detailed analysis of high risks and risk events

Process

- Completing rolling out processes such as risk treatment plan monitoring, KRIs and monitoring, loss event data collecting and analysis, and reporting

- Quantifying high risks and components of value chain, quantify risk correlations, aggregate risks in strategic planning process

People

- Filling CRO position with qualified individual
- Establishing pool model for sharing of risk specialists across businesses/divisions
- Updating job descriptions and developing performance measures for risk related responsibilities for line management and staff
- Implementing continuous learning program for risk specialists

Technology

- Implementing risk treatment plan monitoring, loss event data, KRIs and monitoring plans, alerts and notification, and reposts and dashboards
- Enhancing event tee model to handle multiple time dimensions and expected and unexpected values for market and credit risk
- Developing correlation metrics and incorporating into models
- Developing aggregation capabilities

2.3.2 Risk Assessment

Risk assessment is a holistic process covering risk identification, risk analysis and risk evaluation.

2.3.2.1 Risk Identification

The aim of this step is to be able to generate a comprehensive list of risks based on those events that might prevent, enhance, create, degrade, accelerate or delay the achievement of objectives. Besides identifying the bad risks, it is also important to identify the good risks that are associated with not being able to pursue an opportunity. Comprehensive risk identification becomes critical, any risk that is not identified at this stage may not be included in further analysis but might spring up as a surprise to the management when they are least prepared for it.

The risk identification process involves:

- Conducting workshops at Corporate/plant level
- Conducting Individual meetings with the process owners
- Reviewing the documentation

2.3.2.2 Risk Prioritization

The risk prioritization process would be followed by risk identification phase. It will involve examining the likelihood and impact of an identified risk after determining the existing control measures, if any. Likelihood and impact would be combined to arrive at estimated level of risk i.e. residual risk.

1.1.1.1 ***Total score = Impact * Likelihood***

The risk score of the individual risks identified will be plotted to arrive at the 'HEAT MAP'. The likelihood and impacts will be measured in the scale of 1 to 5.

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

Risk Index:

Once the risk score of the individual risks has been computed, the risk Index for the unit/businesses is computed based on percentage of cumulative risk score against the maximum risk score of the aggregate risk score classified under each category of risks (High; Medium; Low).

Illustration:

Risk Category	*No of Risks*	*Cumulative Risk score*	*Maximum Risk Score*
High	*10*	*124*	*(25 *10) 250*
Medium	*9*	*76*	*(18 * 9) 162*
Low	*54*	*331*	*(10 *54) 540*
	73	*532*	*952*

- **The Risk Index (Cumulative Risk Score/Maximum score) for the Illustrative Unit is 55 %** (532/952 *100)
- Risk Registers would form as the basis to calculate the Risk Index.
- Risk Index will be calculated for the smallest measurable Unit, Business and the Company on a whole.
- Risk Data Analytics to be integrated with the Operational Performance and quantitative measurements inter-alia Risk levels (High, medium & low) to be computed and reported on a quarterly basis.

2.3.2.3 Risk Analysis

The risk analysis process involves:

- Considering the causes and sources of risk

- The events that would trigger the occurrence of risks
- Consequences - positive and negative, the likelihood of occurrence of such consequences
- Severity of impact – monetary, reputational, strategic or operational

The risk analysis aims at identifying the Key Risk Indicators (KRIs). KRI are the factors/ triggers which could lead to the occurrence of the risks which may have direct or indirect impact on the organization. An event can have multiple consequences affecting the objectives. The effectiveness and efficiency of existing controls should be considered while analyzing risks.

2.3.2.3.1 Risk Quantification

Probabilistic Risk Assessment is a formal analytical process method used for risk quantification. Its goal is the developing the methods for predicting or "anticipating" safety concerns before they become manifest through the possible process of:

- Loss
- Injury
- Fatal

NACL adopted Expected Value Analysis to quantify the risk. It's a simple way of determining the severity in risks. To do this we must ensure the probability of 1.0 > 0. Usually, 0.0 and 1.0 are not used since these would mean that the risk would be either an impossibility or a certainty. If the risk is certainty, it should be put into the project plan as a required task; if it is an impossibility, it should be ignored.

The values for the impact of the risks are estimated in dollars or some other monetary value. By evaluating the impact and probability this way, we can multiply the two values together and come up with what is called the expected value of the risk. This value for severity has quantitative meaning. The resulting value is the average value of the risk. In other words, if we were to do this project many times, the risk would happen some of the time and not happen some of the time. The full cost of the risk each time it happens is the impact of the risk. If the probability is less than 1.0, the risk does not occur each time. Adding up the cost of the risk each time it occurred and dividing by the number of times the project was done would give an average value. This is the expected value.

The expected value is extremely useful because it gives us value that could be spent on the risk to avoid it. If the cost of avoiding a risk is less than its expected value, we should probably spend the money to avoid it. If the cost of the corrective action to avoid a risk is greater than the expected value, the action should not be taken.

The expected value of key group risks can be summarized by their expected values into best-case, worst-case, and expected-value scenarios as well. The best-case scenario is the summation of all the good things, but none of the bad things that can happen in the project or subproject. It assumes that all the opportunities will occur but that none of the risks will materialize. The worst-case scenario is the situation that assumes that none of the good things will happen but that all the risks will happen.

2.3.2.3.2 Event Tree

What Are Event Trees?

- A logical sequence of events (triggering events and causal factors) resulting in a loss occurrence that can lead to one or more consequences and impacts

The methodology for developing an event tree requires:

- Break a risk down into its components
- Analyze the risk for each component in terms of trigger events, causal events, conditions, event severity, consequences, and impacts (losses)
- Model the risk components using event tree modeling software/template.

  (Refer to Appendix II for event tree template)

Uses of Event Trees

- Estimate the amount of inherent risk in terms of potential losses
- Estimate the amount of residual risk when assessing and choosing among risk treatment options
- Create comparable risk metrics for a better understanding of the risk profile across business units and risk types
- Create decision support information to be able to take the necessary steps to accept, avoid, transfer, or reduce risk
- Understand and characterize the interactions of risk factors and consequences

Principles for Constructing Event Trees

- Simple enough to be tractable
- Detailed enough to be meaningful
- Acceptable to capture non-quantifiable risk factors if they are important to characterize the risk
- Desirable to capture non-financial impacts if they impact risk prioritization and decision-making

Event Tree Construction

- Identify the major categories of risk factors that could lead to a risk occurrence
- For example, the major categories of risk factors that could lead to an unplanned power plant outage might include plant shutdown or fuel supply disruption
- Identify trigger events or conditions that could lead to the categories

- For example, a fuel supply disruption could be caused by a fuel production interruption, a fuel transportation disruption, or inadequate fuel quality
- Specify the unit of measure for the severity of the risk occurrence
- May incorporate both volume (amplitude of the event) and time (duration of the event)
- Identify the consequences that could result from a occurrence of risk and their impacts
- Capture the impact

2.3.2.4 Risk Evaluation

The risk evaluation process aims at comparing the portfolio of high risks at each entity level with the risk capacity and the risk appetite. The risks identified would be evaluated on quantitative, semi-quantitative and qualitative aspects of impact. The evaluation assists in making decisions based on the outcomes of the risk analysis, evaluation would also throw light on which risks need to be treated besides prioritizing the treatment implementation. Risk evaluation involves comparing the risk levels found during the analysis process against the risk capacity and appetite that were established. Based on that comparison, the need for treatment can be considered.

Decision processes should consider the wider context of the risk and should include the consideration of tolerance levels for the risks borne by the external parties – like business partners and suppliers, who are not part of the organization, but can benefit from the risk. Decision making process should not ignore the legal, environmental, regulatory and other requirements.

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

2.3.2.6 Effective implementation

All the key group risk identified after prioritization, for those Key Risk indicators (KRIs) should be identified and mapped with the respective personnel job function. Periodic reporting frequency is defined for all the risks identified and it should be ensured. Risk assessment is a continuous exercise, and all the key group risks should be periodically reviewed and if any new risks identified the same should be part of monitoring.

2.3.2.7 Risk appetite & Risk tolerance

Risk appetite is the amount of risk on a broad level and entity is willing to accept in pursuit of value. This amount should not exceed the Capacity. **It is determined by the Board that it is 10% of the Net worth of respective business.** It reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style. Risk appetite would generally be used to describe the businesses, markets, products and activities in which a firm would or would not participate, as well as its general philosophy toward variability of returns

Risk Appetite Statement

NACL is a commercially oriented, public company. It recognizes that there are risks inherent in its operations

NACL takes care of the interest of stakeholders and the environment. This results in establishing strong and trusting relationships with stakeholders and supporting the community through activities that foster the economy.

Structured management of risk helps the Company to achieve its objectives. It has different levels of risk appetite for different business activities. Its risk appetite is expressed by the following statements.

- *NACL exploits strategic risks commensurate with the business opportunities.*
- *To deliver high value, NACL knowingly accepts market and credit risks in order to leverage profit upside.*
- *NACL protects its long-term financial strength in order to secure access to capital.*
- *NACL has a low tolerance for risks relating to health, safety, security, environment, fraud and compliance*
- *Risks will be managed on an integrated basis as a risk portfolio across the businesses and risk types.*

Risk tolerance is the acceptable levels of variation relative to the achievement of strategic objectives. Risk tolerance can be measured in the same units as the related objectives. Performance measures are used to help ensure that actual results will be within established risk tolerances. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and provides comfort that the entity will achieve its objectives.

Both risk appetite and risk tolerance are both formal statements to be ratified by the Board and reviewed as and when necessary.

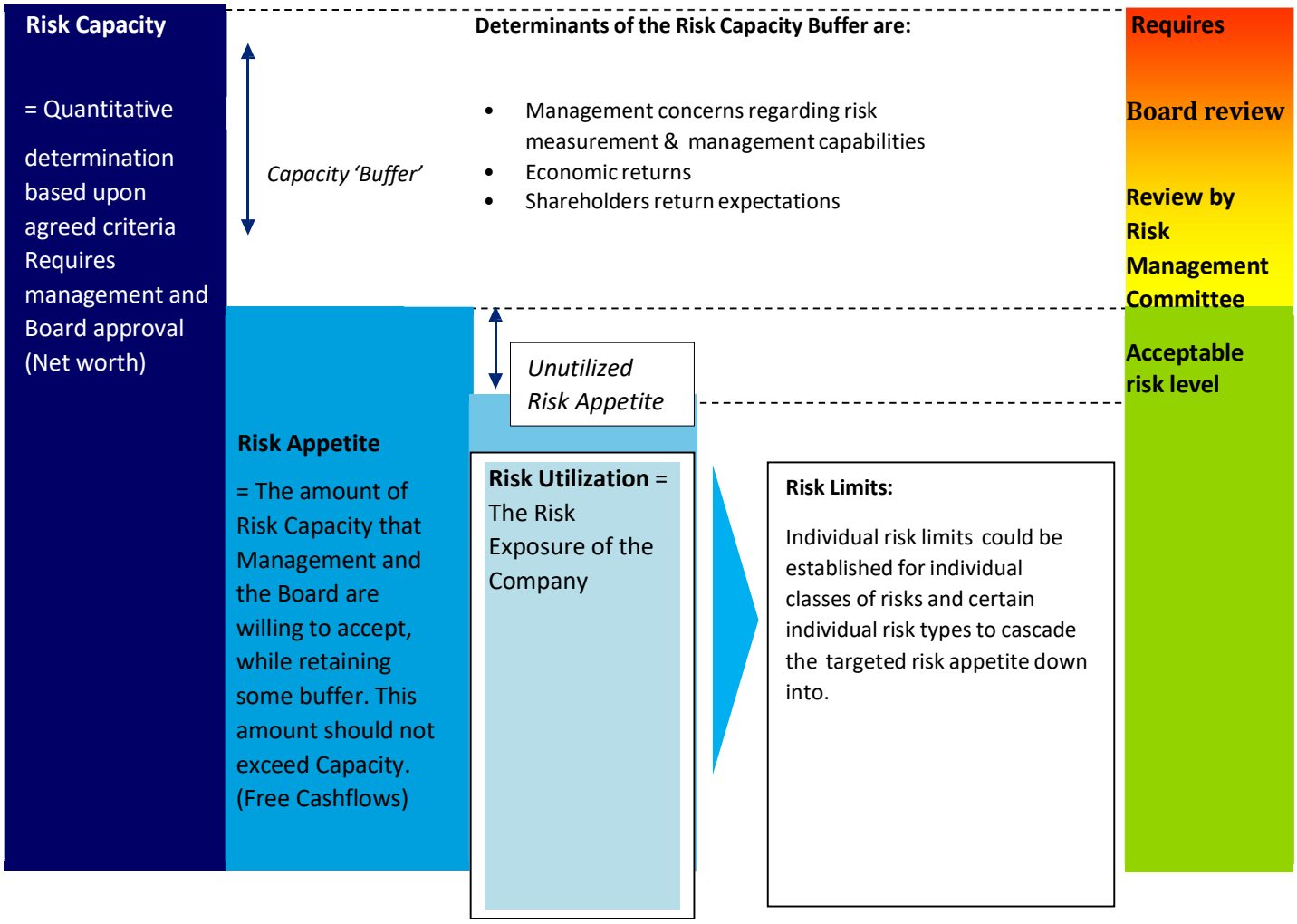


Figure 5: Risk Capacity, Appetite and Utilization

2.4 Risk treatment

The main purpose of risk treatment at this stage is to evaluate the strategic choices against risk factors both good and bad. Risk treatment would involve selection of one or more options for modifying risks, and to implement those options. Once implemented, the treatment would provide a platform for implementation of enterprise-wide risk.

Risk evaluation and treatment should be a continuous and dynamic process that would:

- Assess risk treatment.
- Decide whether residual risk levels (risks that are inherent even after factoring the mitigating controls) are within the tolerable limits.
- In case the risk is beyond the tolerance levels, need to generate a new risk treatment; and
- Assess the effectiveness of that treatment

The scenarios where risks cannot be mitigated, the Company should be ready with an actionable risk response plan.

This analysis will aid the management in taking risk intelligent decisions and enabling the Board to integrate these risks within their strategic decision-making process. The strategy broadly entails choosing from the various options that are available for risk mitigation for each risk that was identified. Thus, the ERM framework aims at providing the management with **a common risk language and tool** that would help make more robust strategic choices.

Following diagram shows the interconnection between the risk treatment process and the decision-making process.

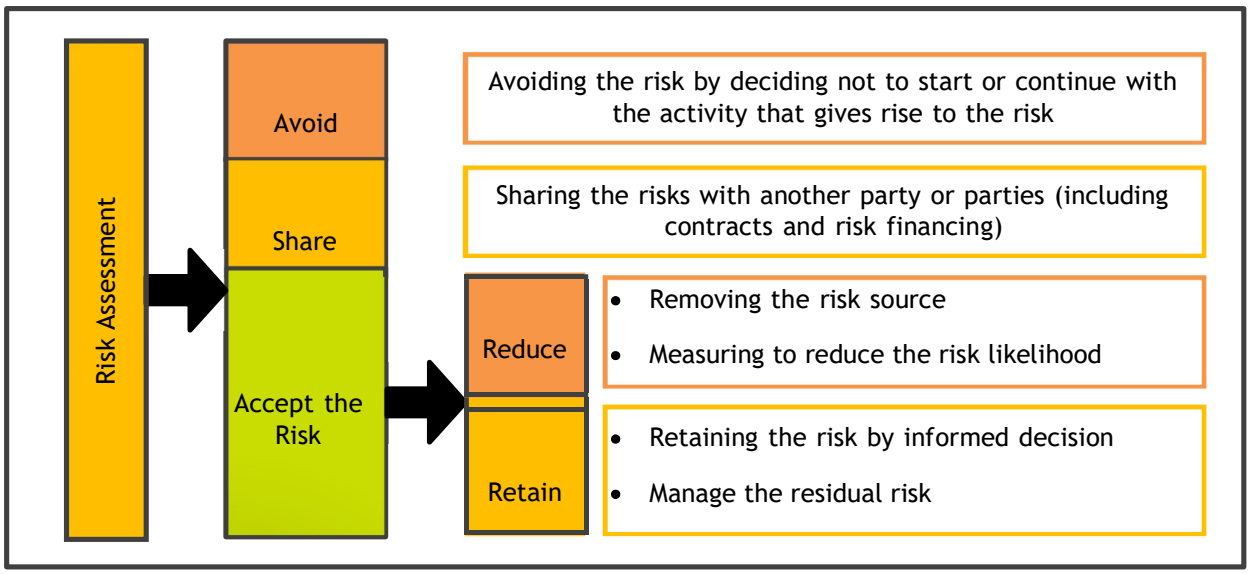


Figure 6: Strategy for Risk Treatment

1. **Avoidance (elimination, withdrawal from or not getting involved)**

   Preventing the occurrence of risk events should be a proactive measure. The risks will emanate as KRIs that need to be continuously measured, monitored and reported.

2. **Reduction (optimize - mitigate)**

   Risk reduction or "optimization" aims to reduce the severity of loss or the likelihood of loss from occurring. Help acknowledge that risks can be either positive or negative, and optimizing risks aims at finding a balance between negative risk and the associated benefits of the activity or operation; and between risk reduction and efforts applied.

3. ***Sharing (transfer - outsource or insurance)***

   Sharing the burden of loss as well as the benefit of gain from the risk (with other party or parties without whom the organization cannot achieve its objectives).

4. ***Retention (accept and budget)***

   Retention involves accepting the loss, or the benefit of gain, from a risk when it occurs. Risk retention provides a viable strategy for those risks where the cost of insuring them would increase over time and exceed the total losses actually incurred. All risks that cannot be avoided or transferred would be retained by default. Such risks could be too large or catastrophic to cover under insurance or demand premium which are not feasible. Those risks with low probability of occurrence but adverse material impact which require exorbitant coverage amounts that can hinder the goals of the organization must be retained.

2.4.1 Monitoring and Review

To ensure effective risk management that continues to support organizational performance and processes, the following needs to be established:

- Measuring risk management performance against the key risk indicators which have to be reviewed periodically for appropriateness of such risks
- Measuring the progress of the risk management process against any deviations from the plan, periodically
- Review the risk management framework, plan and policy for its appropriateness given the external and internal contexts of the organization, periodically
- Reporting – the risks, progress of the risk management plan and remarks captured while implementing the risk management policy
- Tools – analytical and structured scientific

2.4.2 Communication and consultation

The external and internal stakeholders need to be involved at all stages of the risk management process by constantly communicating and consulting them and seeking their feedback to improve the risk management process. Therefore, communication and consultation with the stakeholders need to be planned and developed at an early stage. The communication that would be sent out to the stakeholders should address issues relating to the risk, its causes, its consequences (if known), and the measures for their treatment. Communication and consultation with the external and internal stakeholders have to be effective to ensure that the people identified for addressing the risks are accountable for implementing the risk management process and the stakeholders understand the basis for each decision and the reason for such actions.

2.5 Key Risk Indicators and Key Performance Measures

Key Risk Indicators (KRIs) are measurable management metrics or indicators. KRIs serve to alert staff and management, that a risk profile has or is changing. KRIs are tracked relative to a specified threshold, called risk tolerance.

Trends in KRI values are monitored as well as absolute values. If KRIs are approaching or surpass the risk tolerance threshold, then appropriate personnel are alerted. Responses may include heightened monitoring and the taking of preventive or responsive actions depending on the situation.

KRIs can be leading, co-incident, or lagging indicators of likelihood or exposure. Ideally, leading indicators can be identified and used to provide an early warning system that a risk profile is changing, or a risk occurrence is starting to unfold so that preventive action can be taken.

The risk owners and the local risk committee will review risk factors and consequences and brainstorm indicators that might help anticipate a risk occurrence or loss, monitor exposure, measure the risk, manage the exposure or a loss, or report on the risk and its implications. Monitoring of Key risk indicator for high risks is connected to risk owners PD Matrix.

Criteria for Evaluating Possible Risk Indicators

Effectiveness	**Comparability**	**Ease of Use**
Apply to at least one risk factor or consequence. Be measurable at specific points in time. Reflect objective measurement rather than subjective judgment. Track at least one aspect of the loss profile or event history, such as frequency, average severity, cumulative loss, or near-miss rates. Provide useful management information.	Be quantified as an amount, a percentage, or a ratio. Be a reasonably precise and definite quantity. Have values that are comparable over time. Be comparable internally across businesses. Be reported with primary values and be meaningful without interpretation to some more subjective measure.	Be available reliably on a timely basis. Be cost effective to collect. Be readily understood and communicated.

Each KRI and KPI will have an associated monitoring plan. These will be captured in the ERM information system at the at the unit level and at the corporate level for key group risks.

[Refer Appendix II for KRI to KPI Mapping Template.]

3. KEY SUCCESS FACTORS

The following key success factors are imperative to building a Risk Intelligent Organization. If the key success factors are met, the initiatives will succeed and may yield optimal results.

- Board, Managing Director and CFO sponsorship and buy-in with regard to the value of the ERM program
- Risk Owner and the Head Business units, Head of Functions, and Head of Plants buy-in about embedding risk management in day-to-day business activities using procedures, job descriptions, and performance measures to drive the change
- Financial, IT and human resources availability to undertake the initiatives
- Cross-organizational project interdependencies managed
- Financial impact scales updated to reflect maximum allowable loss in risk tolerance statement in updated the ERM Policy
- Risk impact scales reflect appetite consistent with strategic objective of being highly profitable

4.0 RISK REPORTING

Reporting forms the crux of any process and is critical from a monitoring perspective. The results of the risk assessment need to be reported to all relevant stakeholders for review, to seek their input and for monitoring purposes.

The reporting structure at NACL is given below:

A. The **Risk Unit Owners** would be identified who are required to prepare unit level risk evaluation reports (supported with data and analysis) based on the KRIs of the risks that are included in the risk register on a monthly and annual basis. They should create a risk awareness culture and encourage the employees to be proactive in identifying and reporting risks or triggers/KRIs

Monthly Risk Register Review Report

The Risk Unit Owners and the Site Level Management Committee shall review the Risk Registers and KRIs to review the status of existing risks and identify any emerging/new risks. They should also report on the design and operating effectiveness of the existing controls that mitigate existing risk exposure. 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. Where controls are effective, they should report on the impact and likelihood of the residual risks.

If a new risk or some triggers are assessed to be critical to business or operations of the plant/function/business, the Risk Owner must report it immediately to the Head of the Plant/Head of the Function/Head of the Business unit and the Site Management Committee.

The Monthly Risk Register Review Report shall include:

- Risk movements, if any, (through analysis of KRIs) along with reasons for changes in the impact and/or likelihood ratings
- New high 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
- KRI- KPI mapping prepared for high risks, presented showing, number of times event occurred, action taken against that event and result of that action.

The Risk Unit owner will be responsible for preparing and consolidating the report and the same shall be reviewed by the Site Level Management Committee. Approval sign-off by the Head of the plant/Head of the function/Head of the business unit shall be taken and the report will be shared with the Office of CRO by 18th day following the month 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**. The CRO's office must independently validate where the risk grading has been lowered.

[Refer Appendix II for all the reporting formats]

Annual Risk Database Review Report

The Risk Unit Owners / Site level management committees 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 high 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 CRO's office will be responsible for preparing and consolidating the report at the plant level / Function level / business unit level and the report shall be reviewed by the Site Level Management Committee, business unit management committee and Corporate Management Committee. Approval sign-off by the Head of the plant/Head of the function/Head of the business unit shall be taken and the report will be shared with the Office of CRO as per the schedule detailed in Risk Management Activity Calendar *[Refer section 2.2.3].*

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**. The CRO's office must independently validate where the risk grading has been enhanced.

[Refer Appendix II for all the reporting formats]

B. The **Office of CRO** *[Refer Section 2.2 for detailed roles and responsibilities]* would be required to prepare on a half yearly basis a report for the Risk Management 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 by NACL
- Root causes and mitigation plan for the Key Risk
- Status of effectiveness of implementation of mitigation plans for the high Risks identified till date

C. The **Risk Management Committee** would be required to submit report to the Board on an Annual 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 high risks

[Refer Appendix II for all the reporting formats]

5.0 AMENDMENTS

a) The Company has the right to modify or amend the policy from time to time without any restrictions or explanations, on due adherence of this policy as per the law or any other statutory requirements for the time being in force.

b) In case of any subsequent changes in the provisions of the Companies Act, 2013, or any other regulations or Listing Agreement, which makes any of the provisions in the Policy inconsistent with the Act or regulations, the provisions of the Act or regulations would prevail over the Policy and the provisions in the Policy would be modified in due course to make it consistent with law.

c) This policy shall be reviewed by Risk Management Committee and the Audit Committee as and when any changes are to be incorporated in the

policy due to change in regulations or as may be felt appropriate by the Committee.

d) ***Any changes or modification(s) in the policy as recommended by the Committees would be presented for approval of the Board of Directors.***

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 (PAT)**	**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	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	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	Major breach of regulation; major litigation
5 - Severe	> 15 %	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

LIKELIHOOD CRITERIA DEFINITIONS

	Probability Descriptions		
Likelihood	**Occurrence if future**	**% Likelihood Factor**	**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	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.

Note: Likelihood Factor =Probability (X) Frequency

RISK HEAT 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 soon	**> 12**
MEDIUM	Moderate Risk. Functional Heads attention required	**Between 8 to 12**
LOW	Low Risk. Manage by routine procedures	**< 8**

Note: Impact if 4 or more is treated as High risk irrespective of the likelihood and requires high focus.

APPENDIX - II

REPORTING FORMATS AND TEMPLATES

A. Monthly & Quarterly Risk Register Review Report – From Risk owner to the Site level/Business Unit / Corporate Management Committee / Risk Management Committee and CRO

Monthly Key Risk Review Report					
Month :	Date:	Name of the Risk Unit Owner:			
Risk Register					
Risk Statement:					
Function /					
No of KRIs Identified:					
No of KPI Assigned:					
Details of KPI Owners and monitoring frequency					
S.No	Name of the KPI Owner	Frequency & No of KPI assigned		Occurrence of any event (Yes / No) and KPI Reference	
Risk Unit Owner Signature:					
Function Head Name & Signature:				Date of Review:	
SLMC Chairman Signature:				Date of Approval:	
Date of the SLMC Meeting					
SLMC Coordinator Signature:				Date of Receipt of document:	
Comments if any:					

Monthly KRI-KPI Review Report					
Month :	Date:		KPI Owner:		
Risk Register Reference:					
Risk Statement:					
KRI-KPI Reference		Monitoring Frequency:			
KRI Description					
KPI Assigned					
Whether the Activity Performed	Yes	NO	NA	Supporting document evidencing activity performance:	
If No / Partial, describe the reasons					
Occurrence of any event (After performance of the above activity)				Yes	NO
If Yes, describe the event					
Root cause for the event					
Action performed by the KPI					
Current Status of the Event					
Action proposed for avoiding further					
Additional Information:					
KPI Owner Signature:					
Function Head Name & Signature:				Date of Review:	
SLMC Chairman				Date of Approval:	
Comments if any:					

B. Annual Risk Database Review Report - From Risk owner to the Site level/Business Unit / Corporate Management Committee / Risk Management Committee and CRO

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 Management Committee Meeting held on:							
Chairman of the Site Level Management Committee: <Name>							
(Signature)			(Designation)			(Date of approval)	
Comments:							
Approved by Plant / Function / Business unit Head: <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 Management Committee Meeting held on:		
Chairman of the Site Level Management Committee: <Name>		
(Signature)	(Designation)	(Date of approval)
Comments:		
Approved by Plant / Function / Business unit Head: <Name>		
(Signature)	(Designation)	(Date of approval)
Comments:		
Presented to the Office of Chief Risk Officer		

D. Quarterly/Half yearly High-Risk Report

Present to the Corporate Management Committee/ Risk Management Committee / BOD by the Chief Risk Officer

Quarterly/Half yearly High 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 High Risks as per the previous review:							
Number of High Risks as per the current review:							
Chief Risk Officer							
(Name)		(Designation)		(Signature)			
Comments:							
Presented to the Risk Management Committee							
Corporate Management Committee Meeting held on:							

E. Event Tree Illustrative Template

Event Tree Format

F. Key Risk Indicator to Key Performance Indicator Matching Report

KRI KPI Template

G. Risk Appetite and Capacity

- **Risk Capacity**: Quantitative determination would be based upon agreed criteria. Risk Capacity is the consolidated amount of equity capital & reserves as on March 31, 2025, i.e. INR XXXX Crs.
- **Risk Appetite**: The amount of Risk Capacity that Management and the Board are willing to accept, while retaining some buffer. This amount should not exceed the Capacity. **It is determined by the Board that it is 10% of the Net worth of respective business**

APPENDIX - III

DEFINITIONS & ABBREVIATIONS

TERM	DESCRIPTION
Risk	Risks are events or conditions that may occur, and whose occurrence, if they do take place, has a harmful or negative impact on the achievement of the organization's business objectives. 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 Appetite	Risk tolerance or Risk appetite indicates the maximum quantum of risk which the company is willing to take as determined from time to time in accordance with the Risk Treatment Strategy
Risk Register	A prioritized risk register highlighting the high 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	Repository of all risks that may impact N A C L has been classified under High, Medium or Low depending on the degree of impact and the likelihood ratings. The risks have been classified based on discussions with all the Business Unit heads and Functional Unit heads
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]

TERM	DESCRIPTION
Likelihood	The likelihood of the event occurring expressed as an indicative annual frequency
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]
ERM	Enterprise Risk Management
CRO	Chief Risk Officer
O-CRO	Office of CRO - Risk Office
SBU	Strategic Business Unit
BoD	Board of Directors
CFO	Chief Financial Officer