Nesco Limited

Risk Management Policy and Framework

03 February 2022

Revision history

This document has been reviewed and approved by

Version	Author	Date	Revision	Reason or Change Description	Reviewer and Approved
1.0	Rishab Doshi, CRO	September 2021	Original	NA	Reviewer – CFO, RMC Team Approver – CMD
		03 February 2022	Original	NA	Approved by Board of Directors

Term	Description
AC	Audit Committee
BoD	Board of Directors
CFO	Chief Finance Officer
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
RMC	Risk Management Committee
ROC	Risk Operating Committee

Table of Contents

1. Introduction **4**
1.1. Terms and definitions 4
1.2. Objectives of the Policy 6
1.3. Scope of the Policy 6
1.4. Review and updation of the Policy 7
2. Risk Governance Structure **8**
2.1. Risk Management Organization Structure 8
2.2. Risk Management Roles and Responsibilities 8
3. Risk Management Process **11**
3.1. Risk Identification 11
3.2. Risk Categorization 12
3.3. Risk Assessment 12
3.4. Risk Prioritization 14
3.5. Risk Mitigation 15
3.5.1. Risk Mitigation Strategy 15
3.5.2. Risk Mitigation Process 15
3.6. Risk Monitoring and reporting 16
3.6.1. Early Warning Indicators 16
3.6.2. Risk Review, Governance and Independent assurance 17
3.6.3. Risk Reporting & Communication 18
4. Training, Awareness and Communication **20**
5. Risk Culture **21**
6. Annexure **22**
6.1. Risk Register Format 22
6.2. Risk Card for Identified Risk 22
6.3. Responsibility Accountability Consult Inform (RACI) Matrix 23
6.4. Escalation Matrix 23
6.5. SEBI Guidelines for composition of RMC 23

NESCO LIMITED MUMBAI

1. Introduction

Nesco Limited is a diversified company with business presence in Realty (office spaces), Exhibitions and Events, Hospitality, Manufacturing and Investments. Nesco Limited has established its strategic objectives and recognizes that these strategic objectives will generate risks which need to be assessed, managed, and successfully mitigated so that they do not adversely affect achievement of its strategic objectives. Rapid and continuous changes in the business environment have made it necessary for management to increasingly become more risk focused.

The purpose of Enterprise Risk Management framework at Nesco Limited is to create and protect stakeholder's value by identifying & minimizing the risk exposure and maximizing the opportunities. Risk Management within Nesco Limited shall be responsibility of all employees, and the proactive identification of risks to be actively encouraged and supported. This document lays down the framework of Enterprise Risk Management at Nesco Limited.

An integrated and structured ERM framework shall help the entity to achieve the purpose and benefits in several ways: -

- Identify and manage entity wide risks
- Increase the range of opportunities by managing the risks
- Minimize surprises & negative impact of risks on business objectives
- Encourage an appropriate level of risk tolerance throughout the Company
- Overall resource deployment for managing risks
- Clarity of roles and responsibilities including Board Oversight activities
- Quicker, risk-oriented decisions by focusing on key risks
- Better informed and greater management agreement on key decisions taken
- Achieve business objectives and strategic goals by managing the risk
- Enhanced communication to the Board
- Integrated governance practices
- Ensure risk management framework noticeably respond to the risk profile of the Company.

The Securities and Exchange Board of India (SEBI) has included Risk Management as part of Securities & Exchange Board of India. (Listing Obligations and Disclosure Requirements) Regulations 2015 (LODR) requirement. As per Regulation 17 of the SEBI LODR, disclosures to the Board are to be made by the listed entity on whether the risk assessment and its minimization procedures are in place. As per the Companies Act 2013, there are specific requirements for Risk Management that the company needs to comply with. In addition, the Board of Directors, Audit Committee and Risk management committee have been vested with specific responsibilities in assessing the robustness of risk management policy, process, and systems.

1.1. Terms and definitions

- **Enterprise Risk Management**

  COSO's (Committee of Sponsoring Organization of Treadway Commission) integrated framework defines ERM as:

  "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

- **Risk**

  Effect of uncertainty on objectives

  An effect is a deviation from the expected. It can be positive, negative or both, and can address, create, or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels. Risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood

- **Risk management**

  Coordinated activities to direct and control an organization about risk

- **Stakeholder**

  Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity The term "interested party" can be used as an alternative to "stakeholder".

- **Risk source**

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

- **Event**

  Occurrence or change of a particular set of circumstances

  An event can have one or more occurrences and can have several causes and several consequences.

  An event can also be something that is expected which does not happen, or something that is not expected which does happen. An event can be a risk source.

- **Consequence**

  Outcome of an event affecting objectives

  A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

  Consequences can be expressed qualitatively or quantitatively.

  Any consequence can escalate through cascading and cumulative effects.

- **Likelihood**

  Chance of something happening

  In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

  The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

- **Controls**

  Measure that maintains and/or modifies risk

  Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

  Controls may not always exert the intended or assumed modifying effect.

- **Risk Appetite, Tolerance & Threshold:**

  The risk appetite is quantum / category of risk that the organization is prepared to take / pursue. The threshold is the single point value/ goal/metric and the tolerance is the variation /range/acceptable level in which the risk appetite can be pursued.

- **Risk Residuals:**

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

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

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

  Setting enterprise risk tolerances is a calibration exercise, meaning you need to collect a number of risk assessments for areas known to have high and low risk.

1.2. Objectives of the Policy

The objective of this policy is to ensure sustainable business growth and promote a pro-active approach in identifying, evaluating, reporting and managing risks associated with the business. In order to achieve the key business objectives, this policy establishes a structured and disciplined approach to Risk Management in order to manage risk related issues. The specific objectives of this policy are:

- To enable visibility and oversight of the Board on the risk management system and material risk exposures of the company.
- To ensure all risks across the organization are identified and evaluated through standardized process and consolidated across the organization to identify the key risks that matter to the organization to enable risk prioritization.
- To ensure mitigation plans for key risk are agreed upon, assigned to risk owners and reviewed on a periodic basis
- To ensure that risks are reported at all levels in the organization as per their relevance and significance.
- To ensure that risk governance structure is aligned with organizational structure and risk profile of the company with well-defined and delineated roles, responsibility and delegation of authority.
- To enable transparency of risk management activities with respect to internal and external stakeholders.
- To enable compliance to appropriate statutory & regulatory requirements, wherever applicable, through the adoption of leading practices.
- To assist in defining the early warning indicators and the related leading measures associated to the top risks identified by the enterprise
- To establish and maintain the risk appetite of the organization within the defined threshold levels by tracking the early warning indicators
- Assist in safeguarding the value and reputation by avoiding unpleasant shocks and surprises.
- Validate the implementation of risks management practices and measure the effectiveness using the risk based internal audits

1.3. Scope of the Policy

The policy guidelines are devised in context of the organization's growth objectives, its business and strategy plan, global ERM standards and leading ERM practices. The **Scope of the Policy** shall cover:

- NESCO and its subsidiaries
- All functions at corporate /branch offices
- All events, both external and internal which shall have significant impact on the objectives of the organization

- This policy shall be reviewed by RMC & approved by Board
- This framework and policy shall be reviewed on events such as changes in the business environment/ regulations/ standards, organization structure or upon directives of the Board /Audit committee/Risk management committee

1.4. Review and updation of the Policy

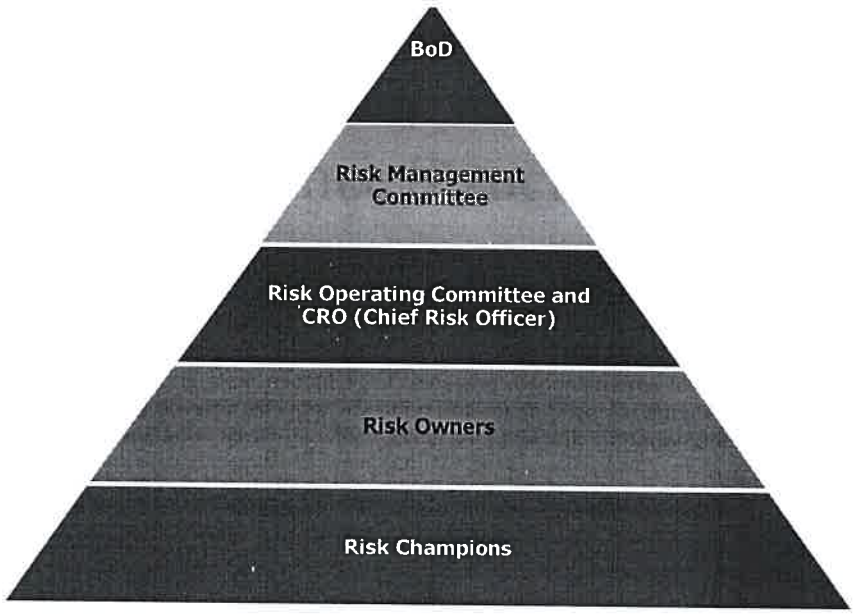
This document shall be reviewed by the Risk Management Committee, once in two years or in case of any significant events such as change in organisation structure, entering or exiting a business segment, change in risk profile, change in government regulations. In the event that the processes defined in this policy are changed, all changes to the existing processes shall be updated and circulated by the CRO. Changed sections shall have a new version number and date

2. Risk Governance Structure

2.1. Risk Management Organization Structure

A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities for the management of risks on a day to day basis. In order to develop and implement an Enterprise Risk Management framework, Nesco shall set up risk management organization structure which will ensure that risk management activities are undertaken as per the policy.

The below chart provides the risk management organization structure within Nesco.



2.2. Risk Management Roles and Responsibilities

Roles and responsibilities for each member within the Risk Management organization structure are detailed below:

- **Board of Directors (BOD)** are entrusted with the key role of ensuring effective risk management and aligning the strategic objectives with the organization's key risks in order to achieve intended outcomes. **Board** shall be responsible for reviewing risk assessment activities, provides strategic input and priority area. However, it may delegate responsibility to Risk Management Committee for administrative purpose

  Key roles and responsibilities:

  - Review and approve risk management policies, guidelines and associated practices on its own and / or as per the recommendations of the Risk Management Committee
  - Oversee the risk management activities are established, implemented and maintained in accordance with the defined framework
  - End to end governance of ERM.

NESCO LIMITED MUMBAI

- **Risk Management Committee** shall monitor and review the implementation of effective risk management Policy & framework including risk reporting, mitigation measures and implementation of action plan. It shall maintain enterprise wide view of the key risks faced by the organization for achieve objective

  Composition of Risk management Committee: The Management shall ensure composition of Risk Management committee is in line with SEBI guidelines issued on 5th May 2021 by SEBI for top 1000 companies (Refer Annexure for SEBI Guidelines)

  Key roles and responsibilities:

  - To facilitate management in formulating Risk Management policy which shall include:
    a. A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks, Business continuity plan or any other risk as may be determined by the Committee.
    b. Measures for risk mitigation including systems and processes for internal control of identified risks.
  - To ensure that risk management methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;
  - To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;
  - To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
  - To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;
  - The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.
  - The Risk Management Committee shall coordinate its activities with other committees (including risk operating committee), where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.
  - Review Risk Management Policy and recommend the same to Board for approval
  - Monitor and evaluate mitigation plan for key risks basis appropriate methodology, processes and systems
  - Monitor the implementation of mitigation strategies for key risks and escalate to the Board and / or Audit Committee, as appropriate.
  - Integrate Risk Management Culture into the Organization
  - Further, RMC has powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

- **Risk Operating Committee** shall include CMD, CRO, CFO and Risk Owners as nominated by the management. As and when the requirement for more departments' representation arises beyond the Risk Operating Committee members in place at the time, the CRO shall invite additional members to join the Risk Operating Committee meetings.

  Key roles and responsibilities:

  The Risk Operating Committee shall have the key role of evaluating the key risks and mitigation measures, monitor and implementation of the Risk Management activities and maintain enterprise wide view of the key risks faced by the organization.

  - Assess and evaluate the key risks anticipated and associated mitigation measures
  - Ensure that effective risk mitigation plans are in place or recommend new mitigation measures as necessary.
  - Guide the risk owners in implementation of mitigation action.
  - Evaluate the Early Warning Indicators for key business risks identified by the Risk Owners

- Discuss the Status of implementation of mitigation measures
- Ensure Ownership of relevant risks are assigned to appropriate Risk Owners

- **Chief Risk Officer** shall work with RMC and Risk owners in establishing and implementation of risk management process effectively in their areas of responsibilities. The CRO shall report to the RMC.

  Key roles and responsibilities:

  - Ensure updation of risk management policy pursuant to the organization's risk management vision
  - Act as convener in Risk Management Committee meetings
  - Validate that the risk management policy is implemented in each department and that all significant risks are being recognized, acknowledged and effectively managed
  - Discuss with risk owners and finalize the ownership of risk registers, thereby entrusting the person with the responsibility of completion of the risk register
  - Coordinate with Risk Owners for periodic update of risk registers
  - Support the Risk Owner in identifying and assessing risks, creating mitigation plans, and development of early warning indicators
  - Report the key business risks faced by the organization and their mitigation plans to the Board on behalf of RMC

- **Risk Owners** are Head of respective function/department/location or business leaders responsible for overseeing the management, monitoring, response and emerging changes related to their assigned risks. They shall be be the point of coordinating and managing all the risk management activities approved by the RMC and BoD.

  Key roles and responsibilities:

  - Ensure that risks for their respective functions/department/location are identified and assessed as per risk assessment framework
  - Understand and take responsibility for the management of risk in their business units/functional areas
  - Ensuring risk registers are maintained and updated on a quarterly basis
  - Ensure effective and efficient coverage of applicable risks
  - Facilitate the identification and implementation of risk mitigation plans
  - Track and measure the effectiveness of the mitigation plans
  - Reporting the risks along with assessment and mitigation of the respective function to the CRO

- **Risk Champions** shall be risk co-ordinators appointed by risk owners within their function (one or more than one) to assist in the risk management activities.

  Key roles and responsibilities:

  - Assisting the Risk Owner in initiating risk identification and assessments within their area of responsibility
  - Taking timely inputs from Risk Owners
  - Compiling risks of the respective business vertical and reporting these to the Risk Owner
  - Quarterly updating and maintaining the risk register for functions as per the inputs from Risk Owners.
  - Assist the Risk Owners in development of mitigation plans

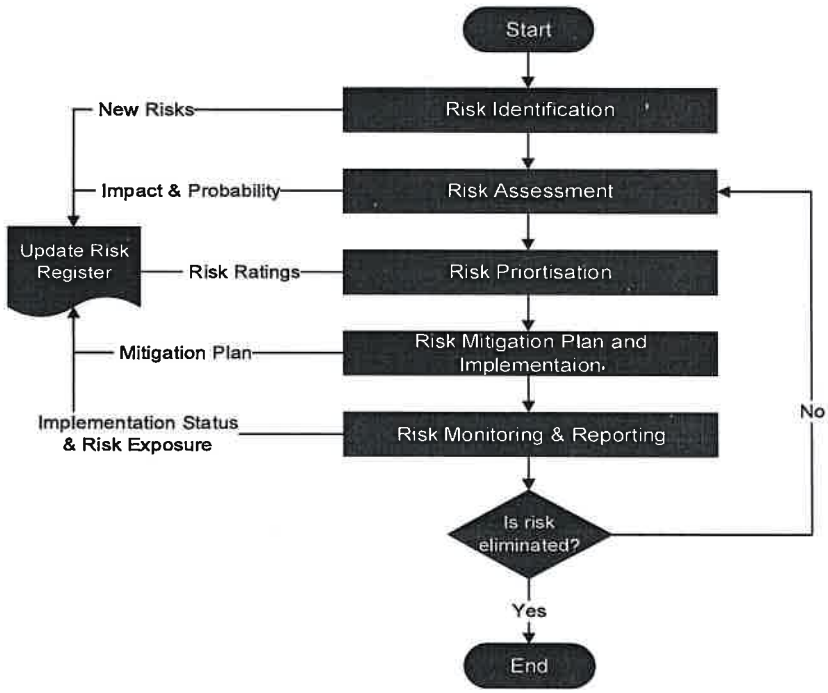
  (Refer Section 6 for RACI Matrix and Escalation Matrix)

NESCO LIMITED MUMBAI

3. Risk Management Process

The risk management process shall be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization.

The risk management process includes following activities: Risk Identification, Risk Assessment, Risk Prioritization, Risk Treatment and Monitoring & Reporting as shown in the figure below:



3.1. Risk Identification

Risk Identification implies finding, recognizing and describing the risks along with identification of their root causes. Risk champions and risk owners to identify and update risk register on a quarterly basis.

The Company is subject to various risks and challenges emerging from the internal environment (e.g. operations, strategy, systems and processes etc.) and external environment (e.g. competition, changes in government policies, Market demand); which may have a significant impact on the organization. Hence, it is important to assess and take action steps in advance to mitigate such risks. Hence, emerging risks form an important part of Enterprise Risk Management process.

Following methodologies and sources to be used for risk identification –

NESCO LIMITED MUMBAI

- Inputs from CXO's or HOD's
- Surveys / Questionnaires
- Structured interviews and brainstorming
- Internal / external audit reports
- Risk Lists - Lessons Learned
- Risk management workshops
- Historical risk event information
- Publicly available risk reports of companies in same industry and industry reports published by reputed organizations

3.2. Risk Categorization

For better risk identification, it is important to know various risk categories. Some sample categories are provided below:

Risk Category	Definitions
Strategic	Potential risks affecting high-level goals, aligned with and supporting the entity's mission/ vision.
Operational	Potential risks affecting the effectiveness and efficiency of the entity's operations. They vary based on management's choices about structure and performance.
Compliance Risk	Risk relating to adherence to relevant laws and regulations.
Financial	Potential risks affecting the performance and profitability goals of the company including safeguarding resources against financial losses.

All emerging risks shall be discussed with the Risk Owners and recorded in the Risk Register.

Refer Annexure 1 for risk register template

3.3. Risk Assessment

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Risk identified shall be classified into internal, external, controllable and uncontrollable and assessed for potential severity as per risk rating parameters.

It is necessary that risks shall be assessed after taking into account the existing controls, so as to ascertain the current level of risk.

Based on the assessments, each of the Risks shall be plotted on a Risk Assessment table and can be categorized as – Low, Medium and High.

The assessment parameters to rate the impact and likelihood of event occurrence of the risk are mentioned in the table below:

Risk Likelihood

Likelihood Assessment Parameters			
Rating	Low	Medium	High

Occurrence	Event may occur only in exceptional circumstances Onset of risk event occurs in a matter of several months No define history of the event	Event could occur in some time or probably occur in most circumstances Onset of risk event occurs in a matter of a few months History of near miss	Event is expected to occur in most circumstances or Very rapid onset of risk event, little or no warning, instantaneous Definite history of occurrence

Risk Impact

Impact Assessment Parameters			
Rating	**Low**	**Medium**	**High**
Financial – Profitability Impact on PAT (INR)	< 2.5 Crores	2.5 Crores – 12.5 Crores	> 12.5 Crores
Financial – Turnover Impact (INR)	< 10 Crores	10 Crores – 25 Crores	> 25 Crores
Financial – Market capitalization	< 5% of decrease	5% - 10% of decrease	> 10% decrease
Legal Compliances	Legal notices and penalties of <INR 10 Lakh	Penalties of INR 10 Lakh or more but <INR 50 Lakhs Warning received Government Enquiry	Penalties of INR >50 Lakhs Non public reprimand or Repeated reprimands Any issue impacting liability of Directors or Potential imprisonment of Directors
Reputation, Ethics & Governance	Credibility affected with regard to specific matter (project / geography) for temporary period Public concern restricted to local complaints	Credibility affected with regard to specific matter for prolonged period Negative Publicity Active news for a period upto 6 months	Overall credibility affected, and ability to influence policy significantly impaired Extended press reporting Active news for a period of ~ 1 year
Management Effort	Middle Management	Senior Management / Functional Heads	Board
People	attrition of non-key employees No effect on ability to attract new talent	Limited attrition of key employees No effect on ability to attract new talent	Loss of key employee(s)/ middle or senior management Affects ability to attract new talent within across business in long term
Business Continuity	Continuity threatened for a minor period	Continuity threatened temporarily	Continuity threatened permanently

Risk appetite shall be defined for identified and potential risks and should considered while formulating strategies, business plans, undertaking business initiatives, managing performance and designing policies. Risk Appetite shall be communicated by the management, endorsed by the RMC and disseminated thought the entity. Risk appetite shall be well informed to all decision makers to understand the risk appetite they must operate within and perform task to achieve the business objective.

3.4. Risk Prioritization

Risk Prioritization is process wherein the overall set of identified risk events, their impact assessments, and their probabilities of occurrences are "processed" to derive a most-to-least-critical rank-order of identified risks. A major purpose of prioritizing risks is to form a basis for allocating resources.

Risk prioritization shall be carried out by Management basis the scoring of the risks.

The impact for a particular risk shall be assessed on the following areas,

- If a particular risk impacts multiple areas, the highest rating will be considered.
- For example, if a particular risk has a 'High' Financial Impact and a 'Low 'Regulatory Compliance Impact, the final impact rating for the risk will be 'High'

The final risk rating can be obtained from the table based on the values assigned against each of the risks identified

Parameters	Low	Medium	High
Likelihood	1	5	10
Impact	1	5	10

Measure of Risk Exposure is given below:

For example, if the

Likelihood is High

Impact is High

The final risk rating is as follows: 10*10 =100

Risk Rating Score	Colour Coding
1-25	Green
25-75	Amber
>75	Red

Based on the "Severity" and "Appetite" of the risk, prioritize the risk for its mitigation

NESCO LIMITED MUMBAI

3.5. Risk Mitigation

3.5.1. Risk Mitigation Strategy

There are four common strategies for treating risk. There is no single "best" response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

Accordingly risk can be avoided, reduced, transferred or shared.

Risk Avoidance: The situation which gives rise to the risk can be avoided by exiting the activities or conditions that gives rise to risk. This is recommended for the risks with high severity.

Risk Reduction: For the risks which cannot be avoided, measures to reduce either the impact of risk or probability of occurrence can be deployed. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either:

- Containment actions (lessen the likelihood or consequences and applied before the risk materializes) or
- Contingent actions (put into action after the risk has happened, i.e. reducing the impact. Must be pre-planned)

Risk Acceptance/ retention: Accept and tolerate the risk. Risk Management doesn't necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The organization shall tolerate such risks that are considered to be acceptable, for example:

- a risk that cannot be mitigated cost effectively;
- a risk that opens up greater benefits than loss
- uncontrollable risks

It is the role of RMC to decide to tolerate of key risk, and when such a decision is taken, the rationale behind it shall be fully documented. In addition, the risk shall continue to be monitored and contingency plans shall be in place in the event of the risk occurring.

Risk Transfer: Transfer the total or partial risk to external party, e.g. Client, Third party Vendor, Sub-contractor, Insurance company, etc. The following aspects shall be considered for the transfer of identified risks to the transferring party:

- Internal processes of the organization for managing and mitigating the identified risks.
- Cost benefit of transferring the risk to the third party.

3.5.2. Risk Mitigation Process

If the risk treatment mechanism selected is risk mitigation or risk transfer for an identified risk than the next step shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also identify new and improved controls.

Identify controls

New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite.

Control activities are categorized into Preventive or Detective based on their nature and timing:

- Preventive controls – focus on preventing an error or irregularity.
- Detective controls – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

Implement Controls

It shall be responsibility of the RMC to ensure that the risk mitigation plans for each function are in place and are reviewed regularly.

3.6. Risk Monitoring and reporting

The Risk Management Committee is the key group which shall work on an ongoing basis within the risk management framework outlined in this policy to mitigate the risks to the organization's business as it may evolve over time.

3.6.1. Early Warning Indicators

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the risks with their mitigation measures shall be updated on a regular basis. This can be updated basis early warning indicators.

Early Warning Indicators are rule based quantitative or qualitative triggers based on multiple sources of information for early identification of potentially harmful scenarios. They have the following characteristics

1. **Rule based triggers -** These are triggers to flag risks early based on rules – that can be quantitative (like sharp increase in resource cost) or qualitative (like change in government policies)
2. **Multiple sources of information -** The triggers could be based on internal information like supplies, labour issues, high attrition etc. or external information like changes in travel regulations, macro-economic developments etc.
3. There are two levels of EWI's defined : -
    - Level 1 (Strategic Level)
    - Level 2 (Operational Level).

In order to control the risks effectively, the frequency of monitoring plays an important role.

In order to enable this practice, the early warning indicators are defined with the following parameters

- Reporting frequency
- Source of Data
- Threshold
- Tolerance Range
- Actual value
- Current Status in -Red, Amber, Green

As per the frequency defined, the Risk Owners shall collect the actual data and measure the current status of the risk appetite

#			Source	Threshold			Risk Status

	Early Warning Indicators (EWI)	Reporting Frequency			Tolerance Range	Actual Value	Within Appetite	Breach within Range	Appetite Range
1	% of clients for which credit risk assessment performed, as per policy	Monthly	Finance Team	100%	5%	100%			
2	% Revenue from High Credit Risk Client	Monthly	Finance Team	<5%	10%	<5%			

#	Early Warning Indicators (EWI)	Reporting Frequency	Source	Threshold	Tolerance Range	Actual Value	Risk Status		
							Within Appetite	Breach within Range	Appetite Range
1	% of clients for which credit risk assessment performed, as per policy	Monthly	Finance Team	100%	5%	92%			
2	% Revenue from High Credit Risk Client	Monthly	Finance Team	<5%	10%	<15%			

3.6.2. Risk Review, Governance and Independent assurance

The Three Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management:

First Line of Defense	Second Line of Defense	Third Line of Defense
• Management Controls • Internal Controls	• Internal Financial Controls • Compliance reporting • Management reporting & review meetings	• Risk based internal Audits • External Audits • Independent Enterprise Risk Assessment reviews

Level 1 : Functions that own and manage risks

NESCO LIMITED MUMBAI

As the first line of Defense, Risk Owners own and manage risks. They shall be responsible for implementing corrective actions to address process and control deficiencies. Risk Owner is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.

Risk Owner shall identify, assess, control, and mitigate the risks, guide the development and implementation of internal policies and procedures and ensure that activities are consistent with goals and objectives.

Risk Champions shall assist the Risk Owner in risk management activities within their area of responsibility and update the risk register for functions as per the inputs from Risk Owners.

Level 2 : Functions and processes to oversee risks

Second line of defense shall be responsible to oversee the overall effectiveness risk management activities along with operations. Second line of defense can be internal or external agencies reviewing control efficiencies through review of

- Periodic performance reviews through MIS and Management Dashboards,
- Compliance to company's policies and procedures
- Compliance to applicable laws and regulations
  - **Monthly Management Reviews-** The Business functions shall perform the self-assessment and publish their dashboard to the function head. Action plans for the critical risk & issue identified shall be implemented with appropriate approvals from the leadership team. This review includes the emerging challenges & constraints as applicable to the respective functions.
  - **Compliance function:** The compliance function shall monitor specific risks such as noncompliance with applicable laws and regulations. Key issues and emerging risks shall be informed to CRO.
  - **Internal Financial Controls Assessment:** Management shall conducts review of internal financial controls to assess the design and operating effectiveness of the controls across the entity. The identified gaps shall be discussed with respective function, and remediation action is identified and implemented for mitigation of gaps. The key findings along with status of gaps and implementation of remediation action shall be reported to the senior management and Board of Directors.
  - **Risk Management committee** shall oversee the overall effectiveness risk management framework and monitor the key risks, mitigation measures and implementation of action plan (covered in section 3 in details)

Level 3 : Functions that provide independent assurance

Third line of defense shall be responsible for conducting independent review of company's risk management activities. Third line of defense includes

- Independent Risk Based Internal Audits
- External audits
- Independent assessment of risk management framework including risk identification, evaluation, mitigation and reporting by third party consultant for periodic basis.

3.6.3. Risk Reporting & Communication

The outcomes of the risk management shall be published & communicated to the relevant stakeholders across the organization. The timely communication of the outcomes enables the relevant stakeholders to take appropriate decisions. The reporting of the risk activities is segmented into 3 levels:-

First Line of Reporting

- Risk Owners shall report CRO with all the risks identified including emerging risk in their respective functions and the status of the Early Warning Indicators on quarterly basis
- CRO shall inform and discuss the key risks/concerns, emerging risks, mitigation actions and status with Risk Operating Committee and if any changes required in risk mitigation plan shall be done and circulated to all stakeholders by CRO.

Second Line of Reporting

- CRO shall convene Risk Management Committee (RMC) meetings shall meet at least twice in a year and not more than one hundred and eighty days shall elapse between two meetings
- CRO shall consolidate the key risks based on the discussion of RMC which shall be reported to the Board.

Third Line of Reporting

- CRO on behalf of RMC shall apprise the board on the key risks faced by the organization and the mitigation measures taken by the management.

(Refer Annexure for Risk Card)

4. Training, Awareness and Communication

In order to increase the knowledge and competency related to enterprise risk management framework and ensure employees understand their responsibility for the management of risk in their business units/functional areas, the following activities shall be undertaken:

- Necessary knowledge awareness and training to the Board regarding the ERM framework and key risks faced by the Company to ensure effective Board oversight
- CRO shall identify the training needs for all employees and stakeholders from risk management perspective and shall conduct periodic awareness sessions for the relevant stakeholders (Including Directors, Risk owners, Risk Champions and Key members of the support function etc.)
- Risk management training shall form a part of employee induction training and to be updated on company intranet
- Management shall communicate the risk culture across organization such as periodic awareness mailers to all employees,

5. Risk Culture

The ability for an organization to successfully achieve its strategy and business objectives depends on organization's core values

- Nesco strives to have open risk culture environment. Different forums such as Periodic Town-Halls, Leadership Town-Halls, Team connect, HR connects, Risk management meetings where employees can understand the existing risks and voice out the new/associated risks/impacts if any to the leadership/management
- Tone at the top to support the desired risk culture of the organization and guide employees to behave in certain desired manner.
- Employees shall be feel free to escalate risk related issues especially when they conflict with the business strategies (Refer Annexure for Escalation Matrix)
- All employees' concerns/ideas to be heard by the Risk owners and acted on
- Middle Management and Functional Managers shall be aligned to company's Mission, Vision, strategies and Risk appetite defined by the management.
- The Board shall oversee the risk culture of the organization periodically and can direct the management to conduct risk culture survey at defined periodically.

6. Annexure

6.1. Risk Register Format

Sr. No	Process	Risk Category	Risk Description	Root Cause	Risk Impact	Risk Likelihood	Risk Score	Overall Risk Grade (H/M/L)	Risk Mitigation Action Plans	Risk Owner	Action Plan Target Date	Action Plan Status

6.2. Risk Card for Identified Risk

Risk Category	
Operational	1

Root Causes

- xx

Mitigation Plans - Existing

- xx

Mitigation Plans - Proposed

- xx

Implications

- xx

KPIs - Proposed

- xx

NESCO LIMITED MUMBAI

6.3. Responsibility Accountability Consult Inform (RACI) Matrix

Activities	Responsibility	Accountability	Consult	Inform
Preparation/ updation of Risk Management Policy	CRO	RMC		Board
Identification Functional / Divisional level risks and preparation of risk register	Risk Champions	Risk owners	CRO	RMC
Facilitate to identify and monitor enterprise level risks	Risk Champions & Risk Owners, Risk Operating Committee	CRO and RMC		Board
Define Mitigation plan	Risk Owners	Risk Operating Committee	CRO	RMC
Implementation of Mitigation actions	Risk Owners	Risk Operating Committee	CRO	RMC/ Board
Appraise Risk Management Committee on ERM Status	CRO	Managing director	-	-
Appraise Board on ERM Status	CRO	RMC	-	-

6.4. Escalation Matrix

Low		Moderate		High	
Immediate	Periodic	Immediate	Periodic	Immediate	Periodic
Risk Champions	Level 1: Risk Owners Level 2: CRO	Risk Owners and Risk Champions	Level 1: CRO / ROC Level 2: RMC	Level 1: Risk Owners and Risk Champions Level 2: CXO's	Level 1: CRO, ROC and RMC Level 2: MD, Vice Chairman and Chairman Level 3: BOD

6.5. SEBI Guidelines for composition of RMC

- The board of directors shall constitute a Risk Management Committee
- Risk Management Committee shall have minimum 3 members
- Majority of members to be the members of board of directors,
- Atleast one independent director to be included in Risk Management Committee
- Meet at least twice in a year and there should not be more than 180 days gap between two consecutive meetings
- The board of directors to define the role and responsibility of the Risk Management Committee.
- Quorum of the meeting to be 2 or 1/3rds of total members of RMC, whichever is higher, Including atleast 1 member of Board

******

NESCO LIMITED MUMBAI