eternal

Risk management policy

eternal

Table of Contents

1. Background

The policy forms part of Eternal Limited's ("Eternal" / "The Company") Internal control & Governance requirements. Also this Policy is in compliance with SEBI (Listing Obligations & Disclosure Requirements), Regulations, 2015 and provisions of Companies Act, 2013 read with Rules made thereunder which requires the Company to implement risk management system. Eternal Limited recognizes that risk management is an integral part of good management practice. The policy explains Eternal's approach to risk management, documents the roles & responsibilities of the Board, Audit Committee, Risk Management Committee, Risk Officers and Risk Owners etc. It also outlines the key aspects of the risk management process. This policy shall operate in conjunction with other business and operating / administrative practices.

2. Purpose/objectives of the policy

The Risk Management (RM) Policy's goal is to establish a formal risk management process within the company to facilitate risk management activities. The management has formed this policy in order to periodically perform risk assessment exercises and to report key risks, Eternal is exposed to, under several categories like strategic, financial, operational, regulatory, reputational, people and technology risks etc. This document demonstrates the commitment of Executive Management within Eternal towards the development, implementation, and maintenance of the risk management program to achieve the following

- To achieve the strategic objective while ensuring appropriate management of risks
- To ensure protection of stakeholder values
- To provide a clear & strong basis, risk informed decision making at all levels of the organization.
- To strive towards strengthening the Risk Management System through continuous learning & improvement

3. Scope

This policy applies to all aspects of Eternal Limited its business lines, support functions and shall cover all stakeholders including but not limited to Eternal's employees, partners, temporary workers, vendors/or service providers. Eternal's ERM Policy covers all the events within the company and events outside the company which have a bearing on the company's business.

Note: If there appears to be a conflict between this policy and applicable laws and regulations or if there are questions regarding the interpretation of applicable laws or sections of the RM Policy, the laws of the country of operation shall prevail.

4. Controls and distribution

The risk management function under Governance Risk & Compliance (GRC) head's supervision is responsible to own, maintain and update this policy and ensure adequacy of this document to cater to the changes recognized in Eternal's business, operating conditions, and regulatory requirements.

The primary copy of this document shall be maintained by the GRC head. Access to this policy by third parties is allowed only with the approval of the GRC head. Such third parties shall sign a standard confidentiality and non-disclosure agreement with Eternal to obtain a copy of this document. Approved amendments shall be communicated to all interested parties where necessary.

5. Administration

- The Risk Management Policy shall be approved by Eternal's Board of Directors (BOD), or its delegate based on the approved delegation of authority (DOA).
- The approved Risk Management Policy shall continue to stay effective until replaced by revised policy, guidelines or is suspended by BOD or its delegate.
- All amendments and new items must be adequately documented and recorded.
- All amendments to this policy shall require the appropriate approval of Eternal's Board of Directors, or its delegate based on the approved delegation of authority (DOA).
- This policy shall be reviewed at least once in two years or in the event of significant business change, including but not limited to:
    - A change in the company's approach to risk.
    - A significant change to internal or external factors o Significant changes in the subsidiary governance model.
    - Legal or regulatory requirements change or introduction of new legislation.
- The Risk Management Policy shall be communicated, understood, and applied within Eternal

6. Principles of risk management

- Risk management is a dynamic and a continuous process.
- A systematic and well-organized approach to risk management is necessary to get consistent results.
- Risk management is integrated/embedded in all organizational activities.
- Risk management framework-process should be tailor made as per its objectives and the internal-external context.
- The Risk Management shall provide reasonable assurance in protection of business value from uncertainties and consequent losses.
- All concerned process owners of the Company shall be responsible for identifying & mitigating key risks in their respective domain.
- The occurrence of risk, progress of mitigation plan and its status shall be monitored on a periodic basis.
- Risk management should involve all relevant stakeholders so that valuable insights are captured and enables in effective decision making.
- Organization culture and human behaviours affects the risk management process.
- Information should be timely, clear and available to relevant stakeholders. The inputs to risk management are based on information that is both historical and current, as well as on expectations for the future. Risk management specifically accounts for any restrictions and uncertainties related to such information and expectations.

7. Definitions

Terms	Definition
Board	Board of Directors of the Company
Committee	Risk Management Committee of the Company.
Policy	means Risk Management Policy.
Risk Register	Refers to the tool for recording the risks identified under various risk units.
Risk	A probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may or may not be avoidable by pre-emptive action.
Risk Management	shall mean the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.
Risk Assessment	shall mean the overall process of risk analysis and evaluation.
Risk Appetite	shall mean the level of risk which an organization is willing to accept, after the implementation of controls, such that there is no significant threat in pursuit of its strategic objectives and value creation
Inherent Risks	The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls). The Risk Management process focuses on areas of high inherent risk, with these documented in the Risk Register.
Residual Risks	Upon implementation of treatments there will still be a degree of residual (or remaining) risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances.

8. Three Lines of Defence Model

- **First Line of Defence**: The first line of defence consists of risk owners for respective business or functional unit. They are primarily responsible for identifying, assessing, and monitoring risks at the functional level. Additionally, they ensure the timely implementation of risk mitigation plans and promote an open and transparent risk culture within their respective units.
- **Second Line of Defence**: The second line of defence is the Risk Management team which reports to Governance, Risk & Compliance (GRC) Head, responsible for implementing, facilitating, and monitoring the risk management process. They also conduct training sessions and workshops, provide clarifications, advice, and guidance to risk owners across business lines and functions on best practices, policies, and procedures related to risk management.
- **Third Line of Defence**: The third line of defence is the Internal audit team which conducts internal audits with the help of external consultants according to the plan approved by the Board. This team reports to the Internal Auditor appointed by the Audit Committee with administrative reporting to CFO. Their role is to ensure that risks are managed within the tolerances established by the Board and that the risk management program is effectively implemented. Internal Audit findings are presented to the Audit Committee of the Board on a quarterly basis.

9. Roles and responsibilities

Board of Directors

The Board, through the Committee shall oversee the establishment and implementation of an adequate system of Risk Management across the Company. The Board shall comprehensively review the effectiveness of the Company's Risk Management system on an annual basis. The Board may re-constitute the composition of the Committee, as it may deem fit, from time to time.

Audit Committee

The Audit Committee shall evaluate risk management systems in Eternal and comment on the adequacy and effectiveness of risk management in the company.

Risk Management Committee (RMC)

The responsibilities of the Risk Management Committee shall be the following.

- Formulate and recommend to the Board a detailed Risk Management Policy which shall include:
    - Framework for identification of internal and external risks specifically faced by the Company, including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the committee.
    - Measures for risk mitigation including systems and processes for internal control of identified risks. o Business continuity plan.
- Ensure that appropriate methodology, processes, and systems are in place to monitor and evaluate risks associated with the business of the company.
- Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- Periodically review the Risk Management Policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.
- Inform the Board of Directors about the nature and content of its discussions, recommendations, and actions to be taken.
- Carrying out such other functions as may be specified by the Board from time to time.
- Any other matter as prescribed by the Companies Act, 2013 & Rules made thereunder, and SEBI (Listing Obligations and Disclosure Requirements) Regulation 2015 or such other Regulation prescribed by the SEBI from time to time.

The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.

The Chief Financial Officer

The key responsibility of a CFO w.r.t Risk Management includes but not limited to:

- Review and provide inputs and recommendations on Risk Management Policy, Risk Appetite and Tolerance and Assessment Criteria and Risk Strategy
- Promote the desired risk aware culture and establish effective risk governance to manage risks across Eternal.
- Facilitate integration of risk management into strategic and business plans and decision making
- Monitor risk management activities on a regular basis through GRC head and help resolve the bottlenecks in a timely manner.
- Review and provide inputs on risk management agenda point, Eternal's risk profile etc. to be presented to Risk Management Committee
- Provide the required budget and resources for managing and implementing the risk management strategy.

Governance Risk and Compliance (GRC) Head

The GRC Head is responsible for overseeing and managing risk managing activities in Eternal as per instruction and guidance from Eternal's Risk Management Committee. The GRC head has administrative reporting to the chief financial officer and has direct line reporting to the risk management committee. The key responsibilities of GRC Head includes but not limited to:

- Developing and maintaining risk management policies and procedures. This involves establishing standards and guidelines for managing risks and ensuring that employees understand and follow these standards.
- Establishing the organization's risk appetite and tolerance levels. This involves setting guidelines for acceptable levels of risk exposure and ensuring that the organization's activities align with these guidelines.
- Developing and implementing risk management strategies that align with the organization's goals and objectives.
- Identifying and assessing risks that may affect the organization. This involves monitoring internal and external factors that may impact the organization and implementing controls to manage the risks.
- Communicating risk-related information to the board of directors, executive management, and other stakeholders. This involves providing timely and accurate information about the organization's risk exposure and the effectiveness of risk management strategies.
- Embracing risk culture across the organization. This involves fostering a culture that values risk management and encourages employees to identify and report risks.
- Ensuring that the organization complies with regulatory requirements related to risk management. This involves monitoring changes in regulations and ensuring that the organization's risk management strategies align with these regulations.
- Monitoring and reporting on the performance of risk management strategies. This involves tracking key risk indicators and reporting on risk management performance to the board of directors, executive management, and other stakeholders.

VP – Risk Management and RM Team

The team under guidance of VP-Risk Management under overall supervision of GRC head is termed as RM Team. The key responsibilities of VP – RM and RM Team includes but is not limited to:

- Review and update Eternal's risk profile on an ongoing basis considering internal and external factors such as change in organizational structure, business objectives, technological advancements, economic conditions, legal and regulatory changes etc.
- Conduct periodic risk assessment exercise in co-ordination with Risk Champions
- Assist Risk Champions in developing risk mitigation plans.
- Identify and monitor Key Risk Indicators (KRIs) for key enterprise risks.
- Report new and emerging risks applicable to Eternal to GRC head along with risk's potential impact on the organization.
- Work with business teams to establish, maintain, and continuously improve Risk Management capabilities, Transfer risk management knowledge through regular training sessions and workshops.
- Provide clarifications, advice and guidance to business lines and functions within the organization on risk management best practices, policies, and procedures.
- Conduct risk management activities in compliance with applicable regulatory requirements.

Internal Auditor

- Conducts internal audits to validate the effectiveness of risk management system and the compliance system based on the applicable risk management standards and methodologies.
- Integrate risk assessment into every stage of the internal audit process to ensure that most significant risks are consistently identified, thoroughly evaluated, and effectively addressed.
- Enhance the effectiveness of audits by ensuring that the audit team focuses on the most critical risks, while also improving efficiency by optimizing audit resources and time spent on high-priority areas.
- The results are reported to the Audit Committee on quarterly basis with suggestion for correction or improvements (if any)

Risk Owners

Each business line or functional head is termed as risk owners for the respective business or function unit. Risk Owners have the primary responsibility to identify, assess and monitor risk at respective function level. The key responsibilities of Risk Owners include but is not limited to:

- Maintain a thorough understanding of Eternal's Risk Management Policy and Risk Appetite ● Ensure adherence with the Risk Management Policy.
- Manage and own all risks within the Business or Functional Units.
- Monitor risk profile of respective business or function units.
- Ensure timely implementation of risk mitigation plans.

- Promote the development of an open and transparent risk culture across their respective business or function unit.
- Identify opportunities for improvement of the risk management framework.
- Ensure effective integration of risk management with business or functional unit strategy and performance.
- Monitor KRIs through Risk Champions

Risk Champions

The key responsibilities of Risk Champions include but is not limited to:

- Support Risk Management team in implementation of Risk Management Policy.
- Facilitate the risk management exercise in respective business or functional unit.
- Facilitate the development of risk mitigation plans with action plan and timelines.
- Ensure the mitigation plans are being implemented as per the agreed action plan and timelines.
- Periodically report the implementation status of risk mitigation plans to respective risk owners.
- Update the risk registers periodically and submit to the Risk management function.
- Report the identified new / emerging risks directly to the risk management department in a timely manner.
- Identify and monitor KRIs for respective business or functional units.
- Undertake training(s) / awareness session(s) in accordance with the risk management training and awareness calendar.

10. Risk management procedures

The stages of Risk Management process are as follows:

a. Risk Identification

This stage entails identifying risk factors, impact areas, events, their causes, and any potential repercussions. The possible event could have a beneficial or negative impact on the company's goals. A variety of strategies are available to the organization for detecting uncertainties that could have an impact on one or more objectives. Following are some points which should be considered -

- causes and events.
- threats and opportunities.
- vulnerabilities and capabilities.
- changes in the external and internal context.
- indicators of emerging risks.
- consequences and their impact on objectives etc.
- limitations of knowledge and reliability of information.
- time-related factors.

Risks must be recorded in a Risk Register that includes details like the risk description, category, categorization, mitigation strategy, and relevant function or department.

b. Risk Analysis

The possibility of each risk happening, and its potential effects are determined through risk analysis. Each detected risk must be evaluated based on two criteria: the impact of an event's occurrence and the likelihood that it will occur. The level of risk exposure is produced by the combination of these two variables.

"Risk Heat Map" is a matrix that may be generated once the impact (consequence) and likelihood of a risk event are calculated.

The potential impact may include -

- Operational impact (People / Technology / Operation)
- Reputational loss
- Regulatory repercussions
- Financial loss.
- Data Security and Privacy
- Legal

The number of prior occurrences in the industry, the audit findings from the prior year, anticipated future trends, or existing research shall be used to rate the risk's likelihood of occurrence (frequency).

Risks must be evaluated to determine the current degree of risk after taking into consideration the controls already in place. Each risk will be rated as Critical, High, Medium, or Low based on the assessments of the risks as per Eternal's Risk Assessment Criteria.

This is further sub divided as mentioned below-

- **Assess Inherent risks –** The risks at inherent level are evaluated assuming there is no control in place.
- **Assess Residual risks –** The risks at residual level are evaluated factoring in the controls in place.

c. Risk Evaluation

"Risk evaluation" involves the comparison of the "risk severity" generated during the "risk analysis stage" with the risk criterion scale (created for both the likelihood and consequence) to determine if any additional action is required. Risks are assessed against the organization's risk appetite to determine their treatment. There could be different decisions which are taken at this level-

- Do nothing further
- Consider risk treatment options
- Undertake further analysis to better understand the risk

- Manage and monitor existing controls
- Reconsider objectives

d. Risk Treatment

The risk treatment is a response to the risk evaluation. While doing risk treatment, it is understood that additional mitigation is needed to reduce the residual risk to a manageable level.
The risk treatment strategies listed below can be used to manage the risk's residual exposure. The best course of action must be chosen by weighing the benefits of additional risk mitigation against the costs, effort, or disadvantages of implementation. It may happen that the additional risk treatment strategy is not feasible in some circumstances; in such a case, the residual risk may need to be accepted and communicated. Risk appetite will also guide the selection of mitigation strategies, ensuring they align with the organization's risk tolerance level

Risk avoidance	By not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.
Risk transfer	Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging / insurance.
Risk reduction	Employing methods/solutions that reduce the severity of the loss.
Risk retention	Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred shall be retained by default.

e. Risk Monitoring and Reporting

To ensure that risks are kept within a reasonable range and that treatment measures have been taken and are working, monitoring of risks and treatment activities should be done on a frequent basis. A planned component of the risk management process with clearly defined roles should include ongoing monitoring and periodic reviews of the risk management process and its outcomes. Successful risk management depends on monitoring and review, thus it's important to specify who is in responsibility of carrying out these tasks. Ongoing monitoring should compare current risk levels with the risk appetite to identify any breaches or adjustments needed.

Risk needs to be continuously re-evaluated in line with the evolving business landscape, changing industry dynamics, and increasing complexities.

A strong emphasis should be placed on identifying emerging risks—those that are not immediately visible but could pose significant threats in the future. This involves monitoring industry trends, staying informed about new regulatory requirements, and leveraging data analytics and external insights to detect early signs of potential risks.

This ongoing risk monitoring and assessment process enhances the organization's ability to protect itself while providing decision-makers with the critical information needed to seize new opportunities and effectively manage potential threats.

f. Communication and Training

To effectively promote a strong risk culture across the organization, regular communication and training programs to be conducted. These programs enhance understanding of risk management principles, raise awareness of potential risks, and foster a proactive approach to identifying and mitigating those risks.

11. Amendment

Any change in the Policy shall be approved by the Board. The Board shall have the right to withdraw and/or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board in this respect shall be final and binding. Any subsequent amendment/modification in the Act or the rules framed thereunder or the SEBI Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

12. Compliance

The Committee would be responsible for supervision of the Policy. All employees of the Company are required to comply with the provisions of this Policy.

Any queries regarding this Policy shall be referred to the authorized person as defined above, who is in charge of administering, enforcing and updating this Policy.

13. Interpretation

In any circumstance where the terms of this Policy are inconsistent with any existing or newly enacted law, rule, regulation or standard governing the Company, the said law, rule, regulation or standard will take precedence over this Policy.

14. Version history

Version	Approved in	Description
Version 1	April 2021	Original Policy
Version 2	May 2023	Updated the Risk Governance Structure
Version 3	February 2025	Following changes have been made ● Clear definition of risk appetite ● Clarity on three lines of defence ● Enhancement of risk management procedures to include emerging risk and communication & training