NHAI InvIT

Enterprise Risk Management Framework,

Policy & Guidelines

Revision	Approval date	Reviewed by	Approved by	Status
1.0	28/06/2023	RMC	Board of Directors	Approved
1.1	02/04/2026	RMC	Board of Directors	Approved

Enterprise Risk Management Framework, Policy & Guidelines

Table of Contents

1.0 Introduction

NHAI InvIT has entered into a Concession agreement with NHAI on 'TOT' basis entitled to rights of Toll collection, Operation and Maintenance of road assets of NHAI for a period of 30 years. NHAI InvIT comprises of following entities:

- National Highway Infra Trust (Trust) – Entity which derives funds from unitholders and funds are invested in SPV for carrying activities related to operations and maintenance.
- National Highways Infra Project Private Limited (SPVs) – Carries activities related to operations and Maintenance of road asset of NHAI.
- National Highway Infra Investment Managers Private Limited (IM)
- NHIT Western Projects Private Limited, NHIT Eastern Projects Private Limited and NHIT Southern Projects Private Limited (SPVs) and future entities

National Highways Infra Trust ("NHIT" or the "Trust") operates through its Investment Manager, National Highways Infra Investment Managers Private Limited ("NHIIMPL" or the "Investment Manager"), and the underlying project SPVs.

NHAI InvIT is exposed to risks related of infrastructure and investment. Unmanaged risk can lead to financial losses, adverse impact on environment & safety, loss of reputation & trust, unintended litigations, and regulatory lapses. These could lead to erosion of unitholders' value and diminishing confidence of various stakeholders in the operations of current and future assets.

The InvIT has identified the need for an efficient, effective and demonstrable Enterprise Risk Management ('ERM') process to help support the vision of the organization, considering the dynamic business environment within which it operates.

Through this document, the NHAI InvIT:

- Mandates its commitment to ERM.
- Seeks to embed ERM into the organization culture by instilling risk management culture in its processes, people and technology.
- Intends to align ERM fundamentals with organizational objectives.

2.0 Background

The document details the process for risk management, including processes to provide visibility, oversight, control and discipline to drive and thereon improve the organization's risk management capabilities in a dynamic business environment.

2.1 Policy Statement

National Highways Infra Trust (NHIT) acknowledges that operating within the infrastructure and trust framework environment naturally involves a range of uncertainties. In alignment with the principles of **ISO 31000**, NHIT is committed to proactively identifying, assessing, and managing these uncertainties to safeguard value and enhance organizational performance. By embedding a structured and forward-looking risk management approach, NHIT aims not only to mitigate potential threats but also to leverage opportunities that support the achievement of its strategic and operational objectives in an efficient, transparent, and resilient manner.

The policy statement aims:

a. To establish an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating, and reporting of all risks, including IT and Fraud Risk.
b. To provide clear and strong basis for informed decision making at all levels of the organization.
c. To continually strive towards strengthening the Risk Management System through continuous learning and improvement and to achieve the objectives of this policy through proper implementation and monitoring.
d. To ensure that new emerging risks are identified and managed effectively.
e. To minimize the risks involved to the extent possible by managing their exposure and bringing them in line with acceptable risk appetite of the company.
f. To put in place systems for effective implementation for achievement of policy objectives through systematic monitoring and effecting course corrections from time to time.

2.2 InvIT Regulation 2014 (Updated December 2025)

a. Reg 18: (Investment Conditions and Distribution) - Risks relating to investment conditions, asset eligibility, cash flow stability and distribution obligations
b. Reg 20: (Valuation) - Valuation, assumptions and estimation risks impacting NAV and investor disclosures
c. Reg 21: (Risk management) - In line to regulation**,** framework ensures robust risk management, strong internal control and trustee oversight

2.3 SEBI (Listing Obligations and Disclosure requirement's) Regulation, 2015 Requirements

NHIT is governed primarily by the Securities and Exchange Board of India (Infrastructure Investment Trusts) Regulations, 2014, as amended from time to time, and the applicable circulars / master circulars issued by SEBI for Infrastructure Investment Trust

The governance, oversight and periodic compliance reporting framework applicable to NHIT operates through the Investment Manager in accordance with the InvIT Regulations, including the applicable governance reporting and disclosure requirements specified by SEBI for listed InvITs

In addition, to the extent applicable, NHIT shall also comply with relevant provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("LODR Regulations") in relation to its listed securities, including continuous disclosure obligations, financial reporting, debt-related disclosures, debenture trustee communication requirements, record date requirements, payment status disclosures and website-based disclosures.

The company, through its Board of Directors, shall constitute a Risk Management Committee. The Board shall define the roles and responsibilities of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit.

a. **Regulation 4 (Governance):** Key function of the board of directors is to ensure the integrity of the listed entity's accounting and financial reporting systems, including the independent audit & that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control and compliance with law and relevant standards.
b. **Regulation 21 (Risk Management Committee):** Board of Directors have been cast with responsibility for formulating a Risk Management Committee which shall be charged with monitoring and reviewing the risk management plan.

2.4 The Companies Act, 2013 Requirements

a. **Responsibility of the Board:** As per Section 134 (3) (n) of the Act, the board of directors' report must include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the Company.
b. **Responsibility of the Audit Committee:** As per Section 177 (4)(vii) of the Audit Committee, the Audit Committee shall act in accordance with the terms of reference specified by the Board which shall, inter alia, include evaluation of internal financial controls and risk management systems.
c. **Responsibility of the Independent Directors:** As per Schedule IV [Part II-(4)] of the Act, Independent directors should satisfy themselves that financial controls and risk management systems are robust and defensible.

2.5 Objectives

The main objective of this policy is to ensure sustainable business growth with stability and to promote a proactive approach in identifying, evaluating, reporting, and managing risks associated with the business. To achieve the key business objectives, the policy establishes a structured and disciplined approach to Risk Management, including the development of Risk Register, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are:

a. To ensure that all the current and future material risk exposures of the company are identified, assessed, mitigated, monitored, and reported.
b. To establish a framework for the company's risk management process and to ensure companywide implementation.
c. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.
d. To assure business growth with financial stability.
e. The effectiveness of Risk Mitigation plans shall be ensured through proper monitoring, evaluation

of outcomes of mitigation plans and to look for the scope of its applicability in other areas in order to achieve overall objective of this policy.

To achieve these objectives, NHIT shall adhere to the following core principles:

a. **Effective Risk Management Process:** The Risk Management Committee constituted by the Board shall have overall responsibility to ensure effective risk management process within the company.
b. **Everyone's commitment**: Every function/ department/ office in the organization shall work in coordination to ensure effective implementation of this risk management policy.
c. **Proactive Leadership**: Risk identification (including identification of the risk of lost opportunities), key risk assessment, risk response and risk monitoring are ongoing activities and shall form an integral part of the company's operations, management, and decision-making process. All the identified risks shall be updated in the central repository.
d. **Transparency and Compliance**: The risk management activities along with the most Significant risks shall be reported and the material failures in mitigation measures shall be escalated through reporting line to the relevant levels of organization structure.
e. **Result Evaluation**: To assess the effectiveness of the Risk Management Policy and its implementation and need for improvement if any.

2.6 Scope and Applicability

The document details the process for risk management, including processes to provide visibility, oversight, control and discipline to drive and thereon improve the organization's risk management capabilities in a dynamic business environment.

Purpose

The purpose of this document is to provide guidelines to establish a comprehensive, aligned, proportionate, embedded and dynamic ERM Framework within the company for effective risk management.

The fundamental objective of the ERM is to ensure that the risks are identified and managed in a prioritized, consistent, effective, and efficient manner at all levels within the company.

To realize the ERM objectives, the company aims to ensure that:

a. Risks are identified, assessed and treated by the organization in a timely manner.
b. The risks are reported and/or escalated to the senior management to initiate necessary risk response plans.
c. The potential impact of identified risks on the organization is continuously monitored and controlled within the risk appetite of the organization; and
d. Risk management activities are not considered in isolation; but rather, they are embedded within the standard business processes, operations, and management decision making process.

3.0 Enterprise Risk Management (ERM) Framework

Risk management will protect and add value to the organization and its stakeholders through supporting the organization's objectives by improving decision making, planning and prioritization by comprehensive and structured understanding of business activity, volatility, and project opportunity/threat. It will provide a framework that enables activity to take place in a consistent and controlled manner. The framework will help in creating an environment in which risk management is consistently practiced across the Company and where Management can take informed decisions to reduce the possibility of surprises. The components of risk management are defined by the InvIT's business model and strategies, organizational structure, culture, risk category and dedicated resources keeping in mind the needs of internal and external stakeholders. An effective risk management framework requires consistent processes for assessment, mitigation, monitoring and communication of risk issues across the organization. Essential to this process is its alignment with corporate direction and objectives, specifically strategic planning, and annual business planning processes. Risk management is a continuous and evolving process, which integrates with the culture of the Company.

An effective Risk Management Framework comprises of:

a. Risk management process; and
b. Risk management organization structure.

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

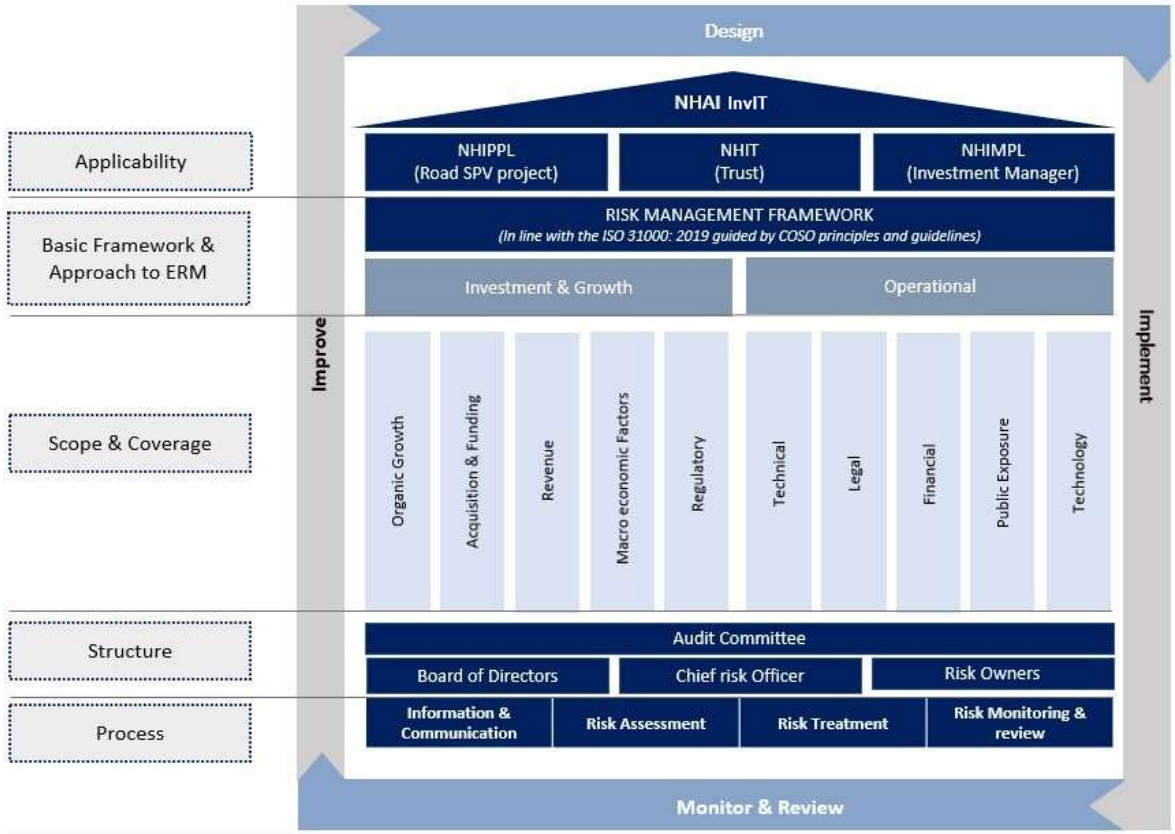
Risk Management Organization Structure: The risk management process has to be supported by a risk management structure which primarily comprises of:

a. Team structure of the Risk Management Function
b. Roles and Responsibilities
c. Risk management activity calendar.

ERM Governance Structure: The InvIT's Risk Management Organization (RMO) structure identifies key internal stakeholders responsible for creating, implementing and sustaining the ERM initiative in the InvIT. The RMO structure leverages existing organizational structure in the InvIT.

The RMO aligns individuals, teams and departments with the intent of establishing responsibility and accountability with regard to:

- Integrating ERM into the InvIT's culture
- Facilitating and monitoring effective implementation of the ERM framework
- Ensuring that the ERM framework and its components are current.



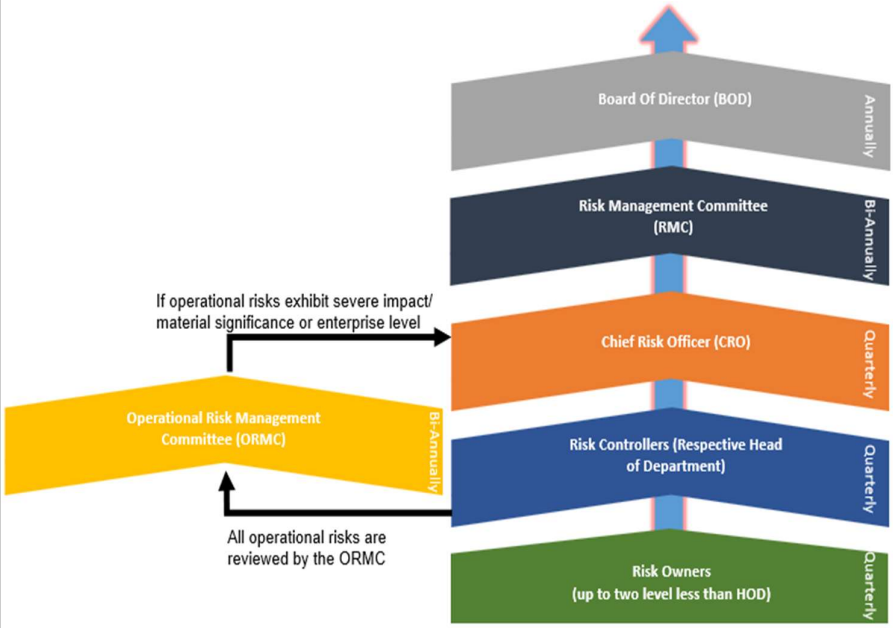
Outside - In approach, wherein the best global Risk Management practices will be benchmarked, and their approach embedded into the company's revised ERM framework.

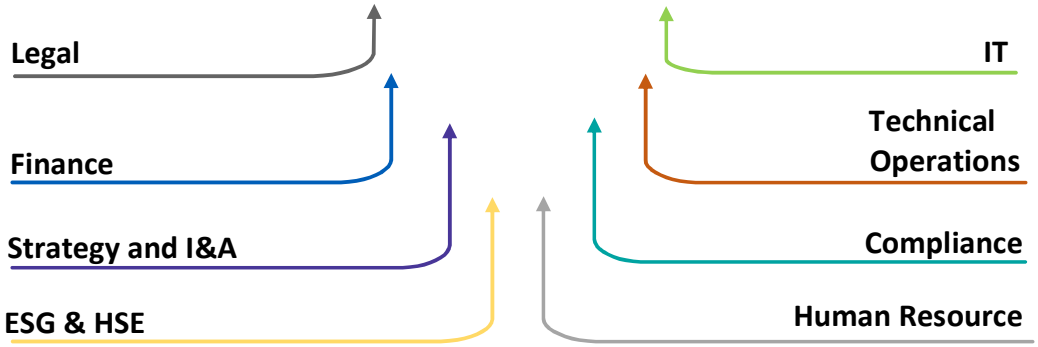
Inside-Out Approach, wherein the internal company stakeholders would be required to provide insights into their respective functions in order to focus on specific risk areas which pose a threat to achievement of company's objectives. This approach would further be broken down into two parts:

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

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

4.0 ERM Governance Structure





Risk Owners
(up to two level less than HOD)

- Department heads to appoint Risk Owners – up to two level less than HOD.
- In cases where employee of required level / designation is unavailable for the formation of Risk Owners, exceptional approvals should be obtained from chairperson of RMC (Director Risk)
- Risk Controllers are to be appointed by each Functional Director of their respective functions (not below Head of Department)

4.1 Roles and Responsibilities

Stakeholder	Roles and Responsibilities
Board of Directors	• Constitute and oversee the Risk Management Committee (RMC) • Periodically review and approve modifications related to RMC Charter • Approve Risk management policy, organization's risk appetite and tolerance levels • Oversee management's response to emerging and strategic risks • Ensure risk disclosures comply with SEBI (LODR)
Risk Management Committee (RMC)	• Review and recommend the Risk Management Policy and risk appetite to the Board for approval • Monitor the organization's overall risk profile and review any significant changes or deviations from the approved risk appetite • Review key risks, associated mitigation measures (adequacy and effectiveness) • Review and approve the Enterprise Risk Registers
Operational Risk Management Committee (ORMC)	• Review operational risk events, incidents, control failures and track mitigation actions • Monitor implementation of risk policies/ processes
Chief Risk Officer (CRO)	• Lead Enterprise Risk Management (ERM) Framework and policy development • Driving risk culture and regulatory compliance • Report periodically to the RMC on the ERM including organization's risk profile, key exposures, and emerging risks • Monitor risk registers and oversees mitigation plans
Risk Controllers (Respective Head of Department)	• Identify and assess risks within their respective departments or functional areas • Maintain and update the departmental risk register, ensuring all key risks, controls, and mitigation measures are captured and managed accurately • Carrying out risk rating and categorization • Implement risk mitigation plans and ensure timely execution of corrective or preventive actions • Escalation of issues requiring policy approvals and amendments to the ORMC/ CRO
Risk Owners	• Comply with Risk policies/ processes/ SOPs and management directives • Keep risk registers updated, implement and monitor mitigation actions • Provide periodic updates on their risks to the Risk Controller and escalate significant issues to Risk controller/ ORMC/CRO

ERM Governance Structure includes a RACI matrix that is defined to ensure clarity in terms of roles and responsibilities of individual stakeholders involved in risk management process. (For detailed roles & responsibilities and RACI Matrix refer to Annexure 1)

5.0 Risk Appetite and Risk Tolerance

Prior to assessing and evaluating the identified risks, it is imperative to understand the concepts of Risk Appetite and Risk Tolerance that help in objectively formulating adequate risk response plans of the organization. The concepts of Risk Appetite and Tolerance Limits are as stated below.

Risk Appetite

Risk Appetite is defined as the type and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. The senior management shall thoughtfully define the risk appetite of the organization to ensure that sufficient value has been assigned towards uncertainties.

Risk Appetite provides insights on the nature and extent of risk acceptable to the company with regards to salient aspects namely projects, services, safety, and compliance in pursuit of value/ achievement of objectives. With the approval of the RMC (Risk Management Committee), the management shall revisit and reinforce risk appetite over time in consideration of new and emerging developments and to ensure risks are managed within acceptable variation.

The risk appetite statements are articulated under three key parameters.

- Financial parameters which provide the threshold in terms of
- Impact on annual budgeted revenue
- Impact on annual budgeted profit
- Impact on budgeted costs/ cost to completion in case of projects in construction stage
- Reputation parameters with respect to specific stakeholders
- Investors, analysts, lenders and rating agencies
- Key customers
- Key vendors/ alliance partners
- Employees
- Media/ general public

Other qualitative parameters have been articulated that set out the appetite regarding.

- Environment, Health and Safety
- Business disruption/ project delays
- Legal issues
- Position with the regulator.

Risk Tolerance

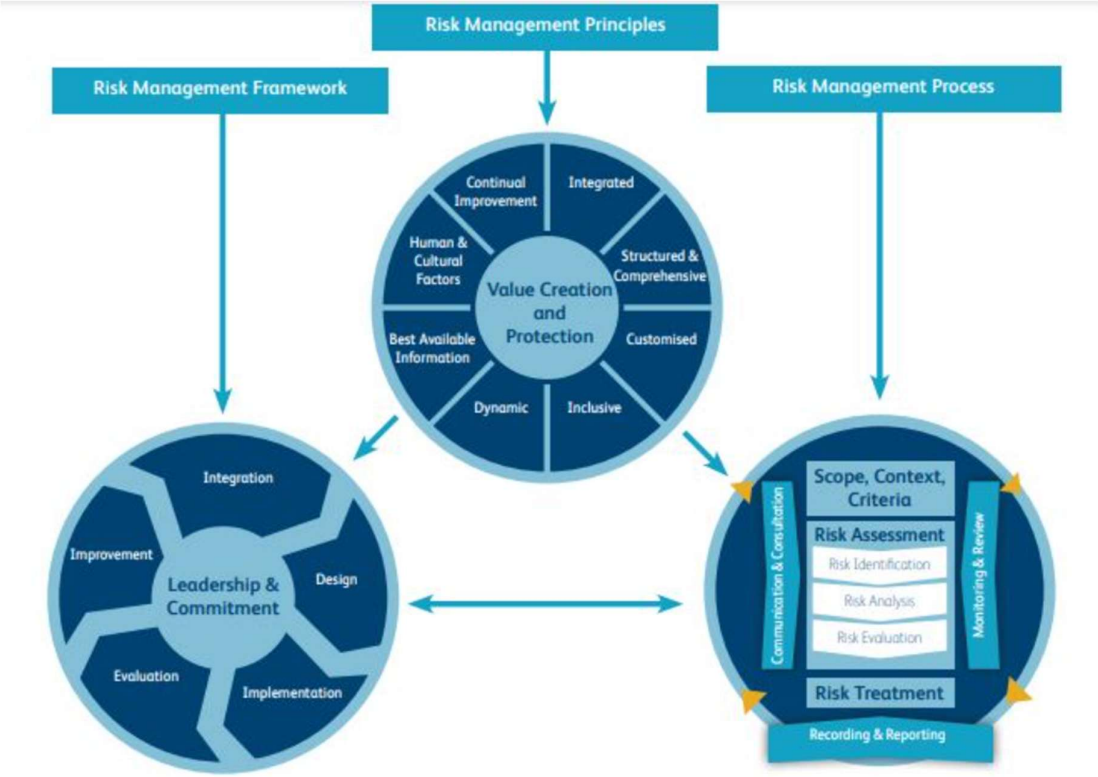
Risk Tolerance is the maximum amount of risk associated with each risk-taking activity that the company is willing to accept in pursuit of its mission, vision and strategic objectives and represents the thresholds beyond which the company is not willing to accept risk.

The risk appetite and tolerance limits shall be determined by the CRO and BoD and subsequently disseminated throughout the organization.

When considering tolerance limits, it is vital to gauge risk acceptability levels by testing these limits with management.

Tolerance limits shall be set based on company's propensity to absorb risk. The risk tolerance levels of the organization are depicted through five (5)-pointer impact scale adapted by the organization to assess risks. The tolerance limits shall be modified based on experience and maturity levels of risk management.

6.0 Risk Management Process



(Source- ISO 31000)

Table 1: Principles of Risk Management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organization.
Aligned	Risk management activities need to be aligned with the other activities in the organization.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organization.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

Effective Risk Management process requires continuous and consistent assessment, mitigation, monitoring and reporting of risk issues across the full breadth of the enterprise. Essential to this process is a well- defined methodology for determining corporate direction and objectives. The risk management framework adopted by NHIT is mapped as per the ISO Standard 31000: Risk Management – Principles

and guidelines and is in-line with recommendations of The Committee of Sponsoring Organizations of the Tread way Commission ("COSO"). Hence, an enterprise wide and comprehensive view will be taken of risk management to address risks inherent to strategy, operations, finance and compliance and their resulting organizational impact.

The Risk Management process adopted by NHIT has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:

a. Establishing the Context
b. Risk Assessment (identification, analysis, and evaluation)
c. Risk Treatment (mitigation plan)
d. Monitoring, review, and reporting
e. Communication and consultation

6.1 Communication and consultation

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

6.2 Establishing the Context

Articulate the objectives and define the external and internal parameters to be considered when managing risk and set the scope and risk criteria for the remaining process. An effective ERM process takes cognizance of both external and internal context in which the InvIT operates. This entails understanding the external environment and internal objectives of the InvIT/Sector/ BU/ Corporate Services as relevant in order to ensure that risks identified are in context of the same.

Establishing the External Context

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

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

- New/ changes in policies/ regulations that may affect the business decisions at a Sector/ InvIT level.
- Supplier InvIT, partners, alliances
- Political scenario at the state and centre in India as well as the scenario in the countries where NHAI InvIT has business interests.
- Economic condition in the states/ countries of operation
- Social factors that may affect the decisions pertaining to a project
- Technological changes applicable to each business
- The social and cultural, political, legal, regulatory, financial, technological, economic, natural calamity/ disaster, and competitive environment, whether international, national, regional, or local.
- Key drivers and trends having impact on the objectives of the organization

Establishing the Internal Context

The risk management process should be aligned with the organization's culture, processes, structure, and strategy. Internal context is anything within the organization that can influence the way risks will be managed. It is necessary to understand the internal context. This can include, but is not limited to:

- Strategy and objectives of the InvIT/ Sectors/ BUs/ Corporate Services
- Inherent strengths and weaknesses/ vulnerabilities of the InvIT/ Sectors/ BUs/ Corporate Services
- Organization structure and expected roles & responsibilities.
- Values & beliefs; Standards, guidelines, and models adopted by the organization.
- Profile of people (qualification/ experience and its relevance to their role)
- Incentive mechanisms and how it is expected to drive behaviors.
- Systems and processes; Policies, objectives, and the strategies that are in place to achieve them.
- Capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies).
- The relationships, perceptions, and values of internal stakeholders; the organization's culture.
- Information systems, information flows and decision-making processes (both formal and informal).

6.3 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment is intended to: Provide the InvIT with an improved understanding of risks that can affect achievement of objectives and the possible business impact of manifestation of risks.

6.3.1 Risk Identification

Risks are events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself. Risk identification is the mechanism of identifying exposure to uncertainty across the InvIT. This involves assessment of the external environment within which the InvIT operates, as well as the internal context of the InvIT, Sectors, BUs and Corporate Services. This stage involves identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

The risk causes, source, events, situations or circumstances which could have a material impact on the objectives of the InvIT, Sectors, BUs and Corporate Services shall also be identified during this phase.
Risks for each operating asset, project, Sector, Corporate Service and overall InvIT shall be documented in individual risk registers. The ownership of these risk registers shall lie with individual Functions; however, the ERM function shall assist in creating and updating the registers.
Risk identification is an ongoing activity. It shall be performed by each employee during the course of his work and particularly at the time of any significant decision, initiation of new Bid/ Opportunity, during project planning and execution and periodically during the life of every operating asset. While the ERM department shall assist in risk identification, it is the responsibility of each function to identify risks. The ownership of these risk registers shall lie with individual Sectors, Bus and Functions; however the
ERM function shall assist in creating and updating the registers. The format for maintaining risk registers

is appended in Annexure 2.

Techniques of Risk Identification

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

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

An event with positive impacts represents an opportunity and an event with a negative impact represents a risk. Risks identified may be of the following types:

- **Strategic Risk:** Competition, inadequate Capacity, high dependence on a on a single customer/vendor
- **Reputational Risk:** Brand impairment, product liabilities.
- **Regulatory/ Legal/ Compliance Risk:** Non-compliance with statutes, change of regulations.
- **Financial Risk:** Liquidity, credit, currency fluctuation
- **Technology Risk:** Innovation and obsolescence
- **Environmental Risk:** Non-compliances to environmental regulations, risk of health to people at large.
- **Personnel Risk:** Health & safety, high attrition rate, incompetence.
- **Operational Risk:** Process bottlenecks, nonadherence to process parameters/ pre-defined rules, fraud risk.
- **Risks arising out of transactions** (Mergers and Acquisitions/Demergers, Restructuring/ sale/ purchase etc.)
- **Information and Cyber Security Risk:** Cyber security related threats and attacks, Data privacy and data availability.
- Other Risk

A brief description of the factors to be considered for categorization of risks is detailed in Annexure 5.

6.3.2 Risk Analysis

Risk analysis involves:

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

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

For example: if at the time of Bid/ Opportunity evaluation, the Business Development Manager identifies a risk which has significant impact on the reputation of the InvIT, the risk maybe escalated to the Project

Team/ CEO relevant. The risk treatment plan can then be decided, which in turn may affect the viability of the Bid/ Opportunity.
A formal risk report containing the "heat map" for the BU, Sector, Corporate Services and the InvIT shall be prepared every quarter as appended in Annexure 4.

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

Risk Measurement: Likelihood * Impact

The risk measurement scale in terms of impact and likelihood has been defined in Annexure 3 – Risk assessment parameters.

Each BU/ Corporate Service function shall arrive at a number of top risks for their respective entities. These top risks shall then be prioritized at the BUs and then prioritized at a Sector level. Similarly, top risks for all Sectors shall be consolidated and prioritized to arrive at a portfolio of top risks for the InvIT.

Risk Rating

Risk category	Score
Low	1-6
Medium	8-12
High	15-25

Risk Rating Heatmap

Risk Matrix					
Likelihood/ Impact	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost Certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

6.3.3 Risk Evaluation

Risk evaluation is the process to determine whether the risk and/ or its magnitude is acceptable or tolerable. The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.
Decisions should take into account wider context of the risk and include consideration of the tolerance of the risks borne by parties, other than the organization, which benefits from the risk. Decisions should be made in accordance with legal, regulatory, and other requirements.

The intent of risk evaluation is to:

- Enable escalation to the appropriate level of Management as per risk measurement criteria.

- Prioritize for treatment implementation.

Risk evaluation helps ensure appropriate resource allocation for the purpose of risk treatment and challenging Management attention towards risks of significant concern.
Risk evaluation will involve risk prioritization for each function and road asset. Risk evaluation shall be done individually and collectively by CRO at various levels.

a. Risk Escalation

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

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

In order to bring risks to the notice of appropriate levels of Management, the process to be used has been depicted in Annexure 5. It is to be noted that at each level of escalation, the risk shall be reassessed so that only the key risks are filtered upwards on a timely basis.

b. Risk Prioritization

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

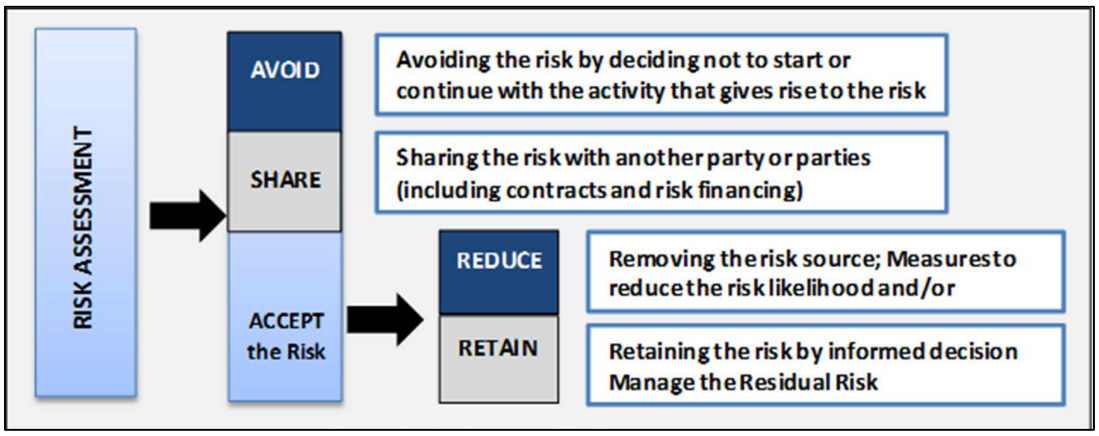
6.4 Risk Treatment

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

Risk treatment involves a cyclical process of:

- Assessing risk treatment.
- Deciding whether residual risk levels are tolerable.
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

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



(Source- ISO 31000)

a. Avoidance (eliminate, withdraw from, or not become involved)

As the name suggests, risk avoidance implies not to start or continue with the activity that gives rise to the risk.

b. Sharing (transfer - outsource or insurance)

Sharing, with another party, the burden of loss or the benefit of gain, from a risk

c. Reduction (optimize - mitigate)

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

d. Retention (accept and budget)

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

6.5 Monitoring and review

All risks recorded in the risk register are reassessed, in order to ensure that risk management is effective and continues to support organizational performance, processes shall be established to:

- Measure risk management performance against the trigger events, which are periodically reviewed for appropriateness.
- Periodically measure progress against, and deviation from, the risk management plan
- Periodically review whether the risk management framework, policy and plan are still appropriate,

given the organization's external and internal context

- Report on risk, progress with the risk management plan and how well the risk management policy is being followed.
- Periodically review the effectiveness of the risk management framework.

6.6 Managing Materialized Risks

In the event of a particular risk materializing, it is necessary to have in place a crisis/ incident management plan for timely and effective management of such events. The incident management plan is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in the InvIT's risk readiness for potentially adverse events.
The InvIT recognizes the need for and shall design such a plan that will detail:

a. The situations for which action plans shall be invoked
b. The manner in which such plans shall be actioned
c. The individuals/ departments involved in such planning and execution

6.7 Risk Reporting

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

Approach implementation at NHIT is as follows:

a. Risk Owners are required to prepare department-wise risk evaluation reports on a quarterly basis and submit them to Risk Controllers for their review:

Quarterly Risk Register Review Mechanism:
The Risk Owners shall submit their evaluation reports to Risk Controllers, and they (after risk owner's responses) shall review the Risk Registers (impact and likelihood of existing risks) and identify any emerging/new risk and the existing control to mitigate that risk. They must ensure robustness of design and operating effectiveness of existing mitigating controls. If required, re–rate (existing risks)/rate (emerging risks) and prepare, implement action plan for risk treatment in situations where the existing controls are inadequate.

The quarterly Risk Register Review Report shall include:

- Risk rating movements, if any, along with reasons for changes in the impact and / or likelihood ratings
- New key risks identified, if any, along with risk criteria ratings and mitigation plans
- Status of the implementation of mitigation plans and reasons for any delays or non-implementations
- Event / events materialized during the quarter that might have triggered any particular risk (not necessarily impacting the risk ratings) along with its mitigation measures.

b. Risk Controllers required to review and approve the department wise risk review reports submitted by risk owners on a quarterly basis.

The Risk owner will be responsible for preparing and consolidating the report and the same shall be reviewed by Risk Controller and then subsequently by CRO.

c. **Chief Risk Officer (CRO)** is required to prepare, on a bi-annually basis, 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 faced by NHIT.
- Root causes and mitigation plan for the risks
- Status of effectiveness of implementation of mitigation plans for the risks identified till date.

Movement in risk rating and new risks identified during each quarter should be duly appraised to RMC on Bi-Annually basis.

Chief Risk Officer (CRO) will be responsible for preparing and consolidating the report for the review, by the Risk Management Committee.

Bi-Annual Risk Register Review Report:
The Bi-annual risk register review report shall include:

- An overview of 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 mitigation plans for the Key Risks identified till date.
- High and Medium risks along with the events that materialized the risk during the period (if any) along with their mitigation plans.
- The risks of having a severe impact, irrespective of their likelihood, shall also be reported.

6.7.1 Risk Management Reporting Timelines

Level of Reporting	Stage of Risk	Timeline	Accountable To
BoD	Reporting to board on risk management in accordance with SEBI LODR, MCA, ISO 31000	Annually	Stakeholders
RMC	Review of the findings of CRO	Bi-Annually	BoD
CRO	Report periodically to RMC	Bi-Annually	RMC
ORMC	Operational risks by Risk owners are reviewed	Bi-Annually	CRO
Risk Controller	Approves risk along with action plan and forwards to CRO	Quarterly	CRO
Risk Owner	Risk owner completes the risk evaluation	Quarterly	Risk Controllers

6.7.2 Change Management

Risk Management ensures identification of risks associated with changes to current business processes/ in external environment

- Changes can be caused by internal events (i.e. internal reorganization or a major corporate initiative) or
- Could be the result of external events (i.e. the impact of new environmental norms or change in regulatory requirement)
- The main difference between the two is the ability of the management to manage the risks that flow from these types of events

A risk assessment should be considered if there is a major change in the way that business is undertaken within the function or if there is a major shift in the operating environment which could significantly impact the function/ operations.

Examples of circumstances where a risk assessment might prove useful, as it will help ensure that all key risks are identified in relation to a specific issue or initiative might include:

- Major changes within the regulatory environment (e.g., Changes in pricing mechanism-WPI (Wholesale Price Index)
- Major changes in the competitive landscape
- Changes are proposed to internal policies and procedures

Criteria for new risk identification/ assessment: Department head should assess and discuss the new risks identified to Chief Risk Officer (CRO) and in turn CRO will present it to RMC for approval depending on the impact on the organization.

Criteria for modification of Risk category: All key risks are assessed and updated by functional heads (in terms of impact and likelihood). All modifications are reported to RMC on periodic basis.

Note: Risk identified/ modified shall be added to Risk Register.

7.0 ERM Approach and Methodology

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

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

Step 2: Collate questionnaire responses and undertake walkthrough of documentation

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

Step 3: Report the results

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

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

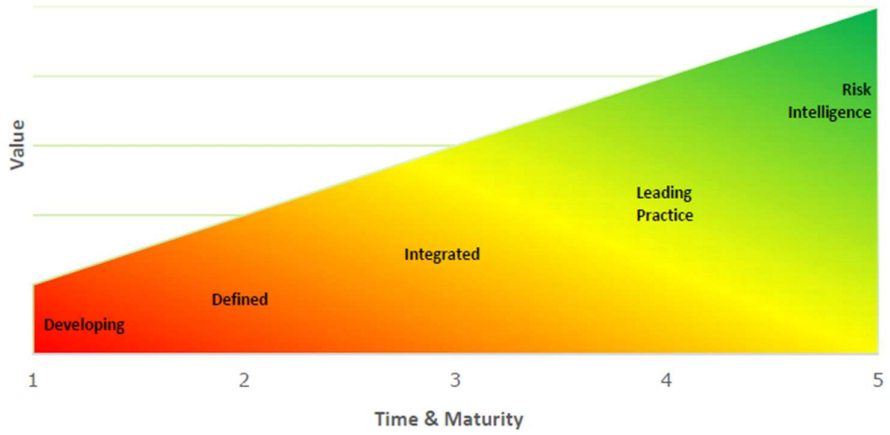
- Basis the importance of the question, specific weights are assigned.
- Based on the 5 stages of the Risk Maturity Model, conclusion shall be made on the current maturity state of the InvIT.

3 pillars of the ERM process, along with Current State Assessment parameters

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

8.0 ERM Maturity Model

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



Time & Maturity

Developing	Defined	Integrated	Leading Practice	Next Gen Risk Intelligent
Activities are unstructured, uncoordinated and undocumented, or they may be absent. No overreaching philosophy / objectives defined.	Most business units function independently. Activities are either not applied consistently across business units or may be in development but are not yet finalized.	Activities are implemented consistently across the enterprise and are correlated and aggregated across risk types (categories) and business units and encompasses most risk types.	Risk is built into decision making. Selectively seize opportunities because of ability to exploit risks	Uses predictive analytics and data driven technologies to automate processes, generate insights and enable risk-intelligent decision making.
• Depends primarily on individual capabilities, and skill set • Limited focus on the linkage between risks. • Independent risk and management activities	• Implementation of additional controls based on identified risk • Reporting on risk exposure • Disparate monitoring and reporting functions • Limited alignment of risk to strategies.	• Common framework, program statement, policy. • Routine risk assessments. • Communication of top strategic risks to the Board. • Executive/Steering Committee. • Knowledge sharing across risks functions. • Functions have ownerships of risks within operations.	• Coordinated risk management activities across silos. • Contingency plans and escalation procedures. • Enterprise-wide risk monitoring, measuring and reporting. • Technology implementation. • Risk management training.	• Embedded in strategic planning, capital allocation, product development, etc. • Early warning risk indicators. • Linkage to • performance measurement/ incentive. • Risk modelling/ scenarios. • Industry benchmarking.

9.0 Document Management

The ERM framework is owned by the CRO. Changes to the document need to be processed through the owner and require the consensus of the NHAI InvIT for ratification.

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

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

Record Retention

For the purpose of ensuring traceability of ERM activities, documentation shall be maintained in physical or electronic form and retained for seven (7) years as per InvIT's Corporate Record Retention Standards.

Records, both physical and electronic, at an Enterprise level shall be maintained by the CRO on behalf of the NHAI

InvIT/ Board of Directors

However, those at the business and Sector levels shall be maintained by individual BU and Sector representative designated for this purpose.

10.0 Annexure

Annexure 1: RACI Matrix

The above roles and responsibilities of key personnel/InvITs within the Risk Governance Structure have been condensed into a RACI Matrix as given below:

Roles & responsibilities	Board	Risk Management Committee	CRO	Functional Owner
Define risk assessment and tolerance levels	I	A, R	I, C	C
Determination of risk impact and likelihood criteria	I	A, R	I, C	C
Identify and Evaluate Department Level Risks	-	I, A	A	R
Aggregate Enterprise Level Risks (Risk Register)	I	A	R	C

* Key risks (critical/severe) are to be discussed by the Board.

Legend:

R- Responsible for undertaking the activity

A- Accountable for making the decisions e.g. Approval etc. for the activity

C- Consulted for input or feedback regarding the activity, agreement not necessarily required

I- Informed about the status of the activity – progress, output, or reports

Annexure 2: Risk Register Format

Risk Register:

Name of interviewees:

Risk#	Risk type / category	Risk description	Root Causes	Likelihood	Impact	Likelihood Impact	Risk Owner	Risk Response	Key Risk Indicators	Comments

Date of interview:

Interviewed by:

Annexure 3: Risk Assessment Parameter

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.

The risk rating for a risk that falls in two or more likelihood / impact parameters, should be treated among the one with the highest likelihood / impact.

Impact Matrix

Sr. No.	Areas	Description	Impact Score				
			1 – Insignificant	2 – Minor	3 - Moderate	4 - Major	5 - Severe
1	Financial Risk	Revenue/ Collection/ Cashflow Impact (per year)	< = INR 1 Cr	> INR 1 Cr - 10 Cr	> INR 10 Cr - 50 Cr	> INR 50 Cr - 100 Cr	> INR 100 Cr
2		Cost impact (per year) – Actual cost > budgeted cost	Up to 3%	>3% - 5%	>5% - 10%	>10% - 15%	>15%
3		Valuation impact (including increase in interest rate)	< = INR 10 Cr	INR 10 Cr - 25 Cr	>INR 25 Cr - 100 Cr	>INR 100 Cr - 250 Cr	> INR 250 Cr
4	Operational Risk	Impact on toll operations (other than force majeure)	Downtime < = 1 day per plaza	Downtime > 1 - 3 days per plaza	Downtime > 3 - 7 days per plaza	Downtime > 7 - 15 days per plaza	Downtime > 15 days per plaza
5		Delay in fulfilment of obligations (including Schedule B) / O&M milestones under the Concession Agreement	Delay up to 10% of duration as per milestone under vendor contract	Delay from 10% to 15% of duration as per milestone under vendor contract	Delay from 15% to 20% of duration as per milestone under vendor contract	Delay from 20% to 25% of duration as per milestone under vendor contract	Delay of more than 25% of duration as per milestone under vendor contract
6		Attrition/ Vacant position % at the following levels: ~Senior Management ("SM") – *{AVP & above}*	SM: No Person MM: No Person LM: 5%	SM: No Person MM: <5% LM: 5 - 10%	SM: No Person MM: 5 - 10% LM: 10 - 15%	SM: 1 to 2 Person MM: 15% LM: 15 - 20%	SM: >2 Person MM: >15% LM: >20%

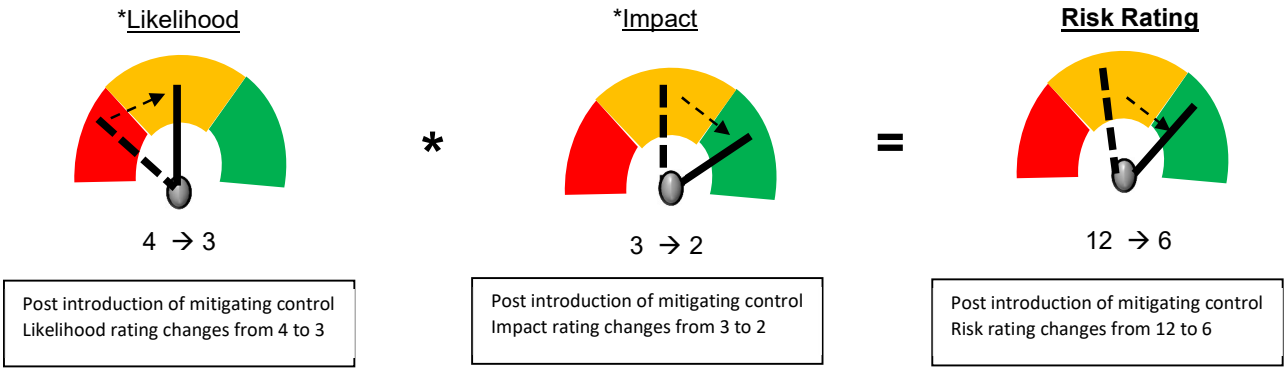
		~Middle Management ("MM") – *{Senior Manager till GM}* ~Lower Management ("LM") – *{Manager & Below}* (Average attrition over last 3 years)					
7	**Compliance Risk**	**Penalties imposed by regulatory authorities/ NHAI (Statutory/ Regulatory or Contractual Compliance)**	Routine issues raised by Ministry / regulatory authorities or Penalty < INR 1 lakh	Warning letter received from statutory authorities or Penalty - INR 1 lakhs to INR 50 lakhs	Penalty letter from statutory authorities between INR 50 lakhs to INR 5 Cr.	Penalty letter by statutory authorities between INR 5 Cr. to INR 25 Cr	Penalty letter by statutory authorities of greater than INR 25 Cr or Possibility of imprisonment of director(s)
8	**Reputational/ Safety Risk**	**Reputation/ Media / Community/ Social**	Minor, adverse local public, and media attention **or** Minor, medium- term social impacts on local population; mostly repairable	Attention from media; heightened concern by local community **or** Ongoing social issues	Criticism by national media/ government Ongoing serious social issues **or** significant damage to structures	Significant adverse national media or national government attention **or** significant damage to structures	Serious public or media outcry; international coverage **or** significant damage to structures
9		**Investors/ Analysts/ Lenders/ Rating Agencies**	No effect on ability to raise funds	Effect on ability to raise short term funds	Effect on ability to raise additional funds	Effect on ability of existing Investor not ready to finance future projects to raise long term funds	Existing lenders/ investors pull out
10		**Health, Safety, Security / Property damage/ Loss of life and/or property due to accidents/ thefts**	Physical discomfort **or** Damage < INR 1 lakh	First aid case **or** damage of INR 1 lakh to 10 lakhs	Temporary disability **or** damage of INR 10 lakhs to 50 lakhs	Permanent disability/ Lost work incident **or** damage of INR 50 lakhs to 1 Cr	Fatality **or** damage > INR 1 Cr

Likelihood

S.No.	Likelihood Criteria	Likelihood Score				
		1 – Rare	2 – Unlikely	3 – Possible	4 – Likely	5 – Almost Certain
1	Probability (In %)	<= 5%	>5% and <= 10%	>10 and <= 50%	>50 and <= 80%	>80%
2	Occurrence in past	Similar instances have never occurred in the past in the industry	Though not routinely but there have been instances in the last 2 to 5 years within NHIT or Industry	There have been one or two similar instances in the past year within NHIT or Industry	Similar instances have occurred in several months (not in all months) in the past year within NHIT or Industry	Similar instances have commonly occurred every month in the past year in NHIT or Industry
3	Occurrence in future	Not likely, almost impossible to occur within	May occur once or twice between 2 - 5 years	may arise once or twice within the next year	may arise in several times (not in all months) within the next year	will be almost a routine instance every month within the next year
4	Pipeline Impact	<5%	5%–10%	10%–25%	25%–50%	>50%
Note: The 'Year' to be counted from the immediate day following the quarter in which RMC meeting is conducted						

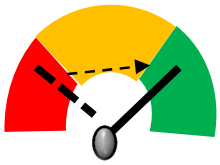
Movement in Risk Rating

Any change in risk rating of risk defined in risk register requires approval of the RMC. Changes in risk can happen due to changes in impact and likelihood of risk. Mitigating control activities would result in changes to likelihood and impact:



Inherent and Residual Risk

- **Inherent risk** represents the amount of risk that exists in the absence of controls. Inherent Risk is typically defined as the level of risk in place in order to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood.
- **Residual risk** is the amount of risk that remains after controls are accounted for. Residual Risk is the remaining level of risk following the development and implementation of the entity's response.



Inherent Risk 16 (4*4) | **Residual risk is 6 (3*2)**

In the above figure, if the inherent risk rating basis impact (4) and likelihood (4) was 16 before a mitigating control in place, the same risk has a residual risk rating of 6, impact (3) and likelihood (2) post introduction of a control activity.

If any new mitigation or control will be mapped against the risk, then subsequently Risk Management Committee will be informed on periodic basis about the movement of risk from inherent to residual rating and the above methodology can be used to show the change in risk rating to Risk Management Committee (RMC).

Annexure 4: Risk Review Report Format

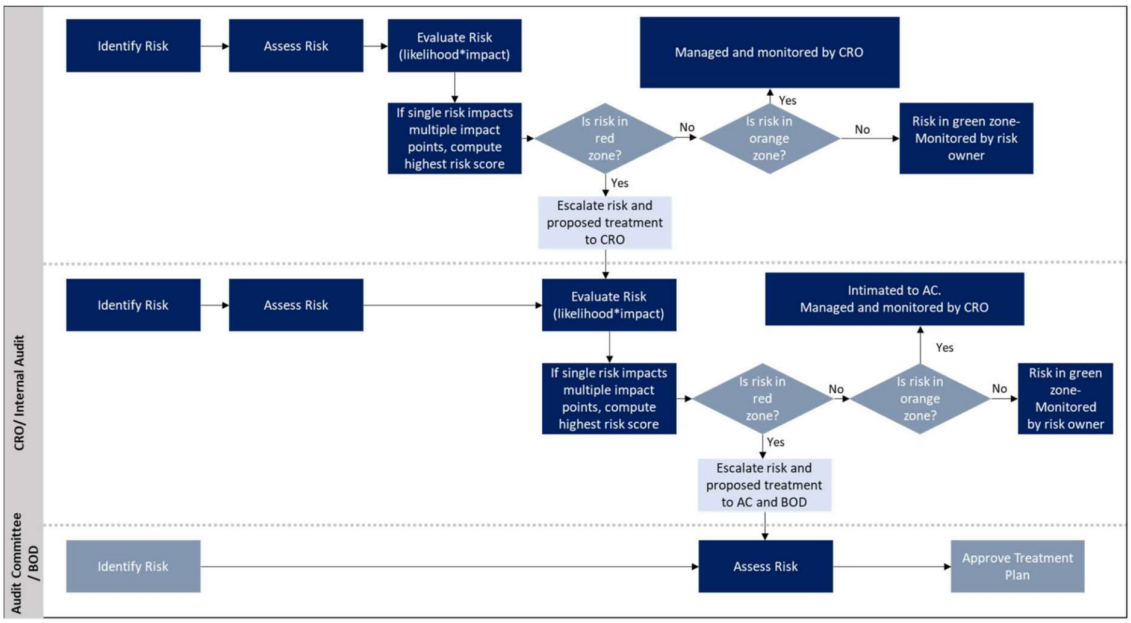
Risk Rating

Risk category	Score
Low	1-6
Medium	8-12
High	15-25

Risk Rating Heatmap

Risk Matrix					
Likelihood/ Impact	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost Certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

Annexure 5: Risk Escalation Process



Annexure 6: Factors to be Considered for Risk Categorization

Categories	Factors
Strategic Risk	• Are the critical strategies appropriate to enable the organization to meet its business objectives? • What are the risks inherent in those strategies, and how might the organization identify, quantify, and manage these risks? • How much risk is the organization willing to take?
Operational Risk	• What are the risks inherent in the processes that have been chosen to implement the strategies? • How does the organization identify, quantify, and manage these risks given its appetite for risk? • How does it adapt its activities as strategies and processes change?
Reputation Risk	• What are the risks to brand and reputation inherent in how the organization executes its strategies?
Compliance Risk	• What risks are related to compliance with regulations or contractual arrangements —not just those that are financially based?
Financial Risk	• Have operating processes put financial resources at undue risk? • Has the organization incurred unreasonable liabilities to support operating processes? • Has the organization succeeded in meeting business objectives?
Information Risk	• Is our data/information/knowledge reliable, relevant, and timely? • Are our information systems reliable?
New / Other Risk	• What risks have yet to develop? (These might include risks from new competitors or emerging business models, recession risks, relationship risks, outsourcing risks, political or criminal risks, financial risk disasters (rogue traders), and other crisis and disaster risks.)

11.0 Risk Vocabulary/ Glossary

Company/Organization: National Highways Infra trust (NHIT)

Board of Directors / Board: As per Section 2 of "The Companies Act, 2013", in relation to a Company, means the collective body of Directors of the Company.

Enterprise Risk Management (ERM): The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk

Risk: According to ISO 31000, risk is the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected. Negative deviations are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. The exposure to the consequences of uncertainty constitutes a risk

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

Risk management framework: Risk Management Framework (RMF) is the structured process used to identify potential threats to an organization and to define the strategy for eliminating or minimizing the impact of these risks, as well as the mechanisms to effectively monitor and evaluate this strategy.

Risk Management Committee: RMC reviews the exception reports along with effectiveness of the mitigation plans and the approval for inclusion/deletion of new risks and modification of the mitigation plans.

Risk Controller: Risk control is a step in the hazard management process. It involves finding a way to neutralize or reduce an identified risk. Risk Controller would be functional level NHIT-wide personnel responsible for moderating responses shared by Risk Owners at a quarterly frequency. The controller would provide feedback to risk owners and share output with CRO.

Risk owner: A risk owner is an accountable point of contact for an enterprise risk at the senior leadership level, who coordinates efforts to mitigate and manage the risk with various individuals who own parts of the risk.

Inherent Risk: Risk level before introduction of any mitigating controls

Residual Risk: Risk level post introduction of mitigating control activities

Events: An event risk is the possibility that an unforeseen event will negatively affect a company, industry, or security

Risk Score: Risk score is a calculated number (score) that reflects the severity of a risk.

Risk Criteria: Risk criteria are terms of reference and are used to evaluate the significance or importance of the organization's risks.

Risk Register: A prioritized compilation under all NHIT Business Units highlighting the key risks for the company.

Trigger Events: Events or conditions that could lead to the risk materializing.

Impact: The degree of consequences to the organization should the event occur.

Likelihood: The likelihood of the event occurring expressed as an indicative annual frequency.

Consequence: The effect, result, or outcome of a potential 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.

Risk Exposure: Risk exposure is the measure of potential future loss resulting from a specific activity or event.

Risk Appetite: Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

Uncertainty: Uncertainties are inherent in all scientific undertakings and cannot be avoided. Proactively managing uncertainties leads to value addition for the company.

Threat: Anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Risk Treatment: A risk treatment is an action that is taken to manage a risk.

Mitigation: Risk mitigation is defined as taking steps to reduce adverse effects.

Risk Identification: Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives.

Risk Analysis: Risk analysis is the process of identifying and analyzing potential issues that could negatively impact key business initiatives or critical projects in order to help organizations avoid or mitigate those risks.

Risk Evaluation: Risk evaluation is the process of identifying and measuring risk.

Risk Governance Structure: The Risk Management Process has to be supported by a Risk Governance / Management Structure which primarily comprises of roles and responsibilities to manage risk across the organization.

Risk Management Plan: A scheme within the risk management framework specifying the approach and resources to be applied to the management of risk; The approach typically includes procedures, practices, assignment of responsibilities, sequence, and timing of activities; and The risk management plan can be applied to a particular product/service, process and project, and part or whole of the organization.

Stakeholder: A person, organization, or entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder.

Risk Tolerance: Risk Tolerance is the maximum amount of risk that an organization is able to absorb in the pursuit of strategy and business objectives.

Establishing the context: “Business context” refers to the trends, relationships, and other factors that influence, clarify, or drive change to an organization’s current and future strategy and business objectives.

Risk Statement: Risk statement is the description of the risk event(s) along with the likely effect/ impact on the organizational objectives.

Risk Assessment: The process of determining the possibility of occurrence of the risk event (Likelihood) and the magnitude of their impact on the organization, which is used to determine risk management priorities basis risk criticality.

Key Risk: Risks which are rated as Severe/Critical would be considered as Key Risk and are Board reportable.

Existing Controls: Existing controls are the measures, if any, already in place to control the risks. These controls are to be evaluated periodically to ensure they are effective.

Response Plans: Response plan is the process of developing actions to eliminate or reduce the frequency, magnitude, or severity of exposure to risks, or minimization of the potential impact of a threat or warning, in consideration of existing controls.

Risk Monitoring: Check, supervise, observe criticality or measure the progress of risk management activity on a regular basis in order to identify change from the performance level required or expected.

Risk Reporting: Form of communication intended to address internal or external stakeholders to provide information regarding the current state of risk and its management.