3i INFOTECH LIMITED

Risk Management Policy

Version 2.O

TABLE OF CONTENTS

1) INTRODUCTION:

3i Infotech Limited ("the Company") has emerged as a leading name in propelling the current wave of digital transformation initiatives, with deep domain expertise across BFSI, Healthcare, Manufacturing, Retail and Government sectors. The Company's business and its presence across geographies exposes the Company to various risks inherent to such business and industry. Accordingly, Risk management is being put in place, to respond to various risks that pose against the Company.

3i Infotech Ltd. is committed to a structured approach in managing key risks and opportunities to maximize shareholder value. This risk management policy outlines the objectives and essential elements of risk management within the organization, fostering risk awareness among employees and embedding risk management into the corporate culture. By systematically identifying, assessing, monitoring, and reporting risks, 3i Infotech Ltd. ensures proactive management of potential challenges, allowing more focus on strategic growth and value creation.

In compliance with applicable requirements of the Companies Act, 2013 and the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, this Risk Management Policy ("Policy") is being formulated by the Board of Directors of the Company.

2) APPLICABILITY:

This Policy shall be applicable to all areas of operations of Company and its Indian and foreign subsidiaries (including step-down subsidiaries).

3) OBJECTIVES:

The objective of this Policy is to effectively manage and mitigate the risks associated with the Company's business activities, while maximizing opportunities and minimizing potential adverse impacts. This will be achieved through:

i) Systematic identification, assessment, and management of risks, with clearly defined ownership and responsibilities.

ii) Ensuring a balanced approach between the cost of risk management and the anticipated benefits.

iii) Contributing to the more efficient allocation and utilization of capital and resources.

iv) Promoting a proactive and forward-thinking approach to risk management across the organization.

4) DEFINITION:

- **Risk:** Risks are potential events or conditions that, if they occur, may have a negative impact on achieving the organization's business objectives. The possibility of adverse outcomes due to uncertainty constitutes a risk.
- **Risk Appetite:** Risk appetite represents the maximum level of risk the company is willing to take, as determined periodically in line with the company's Risk Strategy.
- **Risk Assessment:** Risk Assessment is the complete process of analysing and evaluating risks.
- **Risk Management:** Risk Management is the systematic process of identifying, quantifying, and managing all risks and opportunities that could impact the achievement of a corporation's strategic and financial objectives.
- **Risk Register:** A Risk Register is a centralized document that records, assesses, and tracks potential risks, including their impact, likelihood, and mitigation measures.
- **Risk Strategy:** The Risk Strategy outlines the company's approach to managing various business risks. It includes decisions on risk tolerance levels and the acceptance, avoidance, or transfer of risks faced by the company.

5) RISK APPETITE:

A critical element of the Company's Risk Management Framework is the risk appetite, which is defined as the extent of willingness to take risks in pursuit of business objectives. The key determinants of risk appetite are as follows:

i) Shareholder and investor preferences and expectations.

ii) Expected business performance (Return on capital).

iii) The capital needed to support risk taking.

iv) The culture of the organization.

v) Management experience along with risk and control management skills.

vi) Longer term strategic priorities. Risk appetite is communicated through the Company's strategic plans.

The Board and management monitor the Risk appetite of the Company relative to the Company's actual results to ensure an appropriate level of risk tolerance throughout the Company.

6) RISK MANAGEMENT FRAMEWORK:

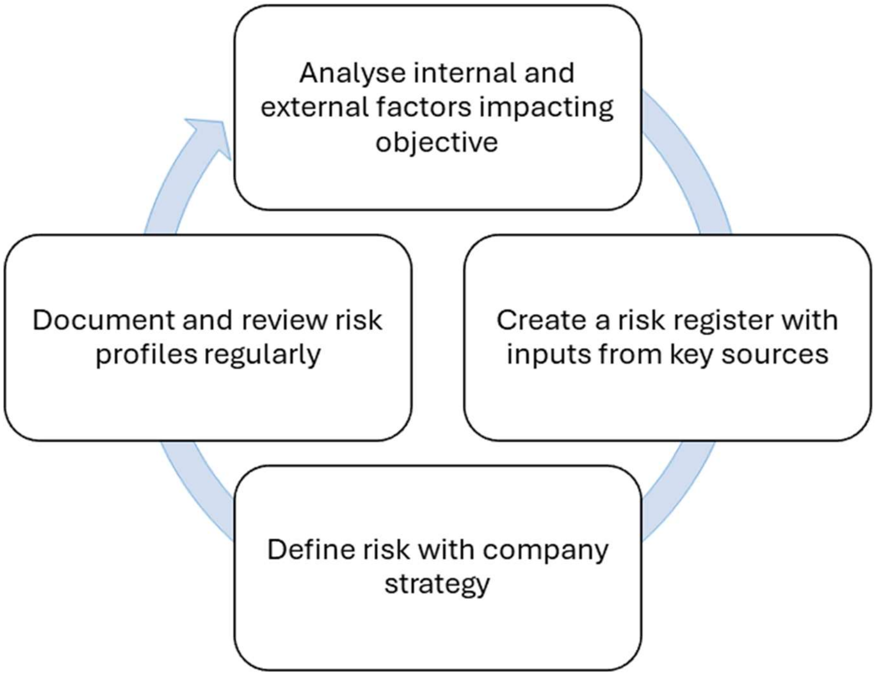
This process involves conducting an annual risk refresh to update the Risk register and assess the progress of action plans, with comprehensive reporting to key stakeholders. The components of Risk Management vary by organization and are shaped by factors such as the company's business model, strategic goals, organizational structure, culture, risk appetite, and available resources. A robust Risk Management process requires continuous identification, prioritization, mitigation, monitoring, and communication of risks across all levels of the organization. It is critical that this process aligns with the company's overall strategic direction, including its strategic planning and annual budgeting cycles.

The Risk Management framework encompasses the following core activities:

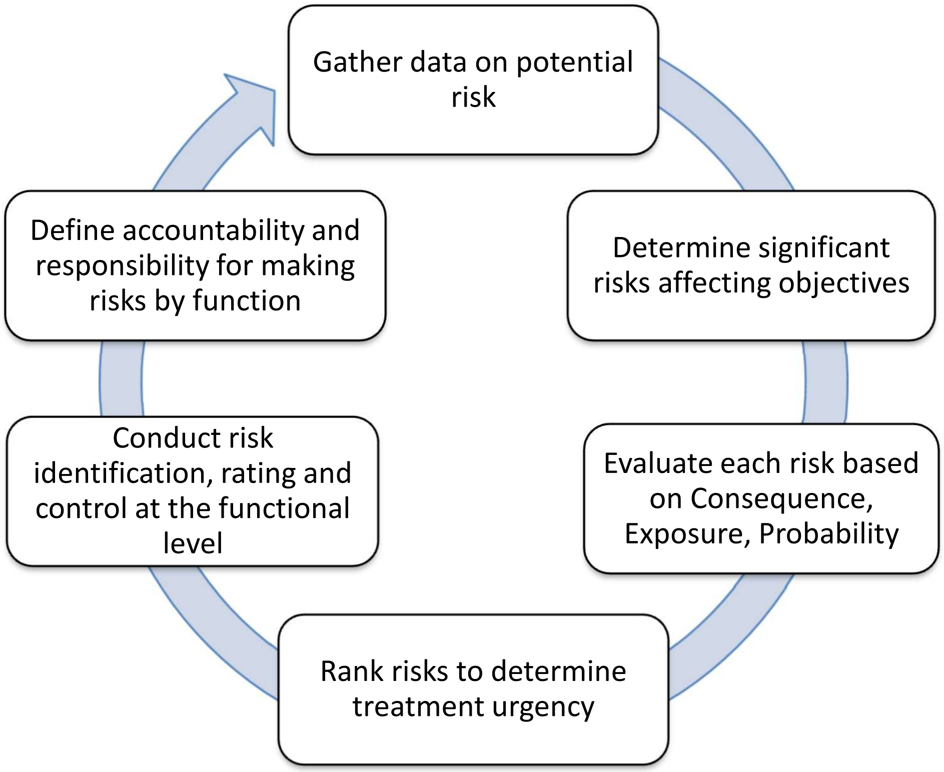
- Risk Identification
- Risk Assessment
- Risk Mitigation
- Risk Monitoring and Continuous Assessment

Establishing acceptable risk levels that are aligned with the company's growth and return objectives are essential to ensure effective monitoring. However, the Risk Management framework is not designed to provide absolute assurance against failure to achieve business objectives or to prevent material misstatements, losses, fraud, human errors, misjudgements in decision-making, or violations of laws and regulations.

i) **Risk Identification:** This step assesses internal and external contexts to identify potential threats to business objectives. A risk register is developed using insights from management discussions, audits, and industry reports. The company defines risks in line with its strategy, documents material risks, and regularly updates risk profiles to ensure alignment.


Analyse internal and external factors impacting objective
Create a risk register with inputs from key sources
Define risk with company strategy
Document and review risk profiles regularly

ii) **Risk Assessment:** Risk assessment and prioritization help determine which risks need treatment and in what order. This involves analyzing each risk’s impact, likelihood, and attributes to identify priority actions. Key steps include gathering information, identifying major risks, rating and prioritizing them, and defining functional responsibilities for effective risk management.


Gather data on potential risk
Determine significant risks affecting objectives
Evaluate each risk based on Consequence, Exposure, Probability
Rank risks to determine treatment urgency
Conduct risk identification, rating and control at the functional level
Define accountability and responsibility for making risks by function

iii) **Risk Mitigation:** The company's Risk Management Strategy, based on assessment and prioritization, involves selecting appropriate mitigation options for each identified risk. A mitigation plan is created for prioritized risks, with assigned Risk Owners responsible for implementation and reporting.

Preventive controls are put in place to avoid risks from occurring in the first place. These controls aim to reduce the likelihood of identified risks materializing by addressing root causes and implementing safeguards. Examples include regular employee training, process improvements, and system safeguards.

Detective controls focus on identifying risks or issues as soon as they occur, minimizing the impact of the risk event. These controls are implemented to monitor systems and processes, allowing for quick detection and response to emerging risks. Examples include continuous monitoring, audits, and anomaly detection systems.

Annual analysis of financial impacts, risk likelihood, and mitigation costs, alongside the integration of preventive and detective controls, guides the strategy. This ensures that there are options to **avoid**, **reduce**, **share**, or **retain** risks, while preventing potential issues and detecting them promptly should they arise.

Risk Mitigation strategy:

- Avoidance: Avoid or eliminate the risk.
- Reduction: Mitigate or control the risk.
- Sharing: Transfer risk through outsourcing or insurance.
- Retention: Accept the risk with an action plan.

iv) **Risk Monitoring and Continuous Assessment:** The company's risk management framework must include effective controls and continuous monitoring to ensure timely identification of significant changes in risks or their mitigation strategies. Since the internal and external environments are constantly evolving, the risk management process should remain flexible to accommodate new challenges. Regular risk reporting, generated by the Chief Risk Officer, ensures that key risks, control measures, and risk indicators are communicated to the Risk Management Committee and Senior Management.

7) RISK PROFILE:

A risk profile is fundamental to an organization's strategic and operational management. It serves as a structured approach that enables the organization to identify and address risks across its activities, aiming to optimize the benefits derived from these endeavors. This process increases the likelihood of achieving success, while simultaneously reducing both the chances of failure and the uncertainties associated with meeting the organization's overall objectives.

The Company focuses on several internal and external risks, including but not limited to:

i) Business risk:

These concern financial loss or operational setbacks arising from strategic missteps, poor business decisions, market competition, or operational inefficiencies

ii) Operational risks:

These concern the day-to-to-today issues that the organization is confronted with as it strives to deliver its strategic objectives.

iii) Legal & Compliance risks:

These concern the legal penalties, financial loss, or reputational damage due to non-compliance with laws, regulations, or contractual obligations.

iv) **Financial and Reporting risks:**

These concern the financial transactions entered into by the organization in domestic as well as foreign currency. It involves threats to financial stability, such as market volatility and credit risks, and inaccuracies in financial reporting due to errors, fraud, or weak controls, potentially affecting compliance and stakeholder trust.

v) **Technological risks:**

These concern operational disruptions, data breaches, or financial loss due to technology failures, cyber threats, or inadequate IT infrastructure.

8) ROLES AND RESPONSIBILITIES:

i) **Board of Directors:**

The Board of Directors (Board) of the Company is responsible for reviewing and ratifying the risk management structure, processes and guidelines, which are developed and maintained by the Risk Management Committee.

ii) **Risk Management Committee:**

The Board has constituted a committee named the Risk Management Committee (RMC), for carrying out oversight and management of risk management program across the Company. The RMC oversees risk mitigation strategies, ensures proper monitoring systems are in place, and regularly reviews the risk management policy. It keeps the Board informed, oversee the CRO's functioning, and foster a risk-aware culture aligned with organizational goals. Additionally, the RMC conducts annual risk assessments and ensures alignment of risk management across business units.

The RMC is inter alia responsible for -

- Devise and implement risk mitigation measures, including internal controls and business continuity plans.
- Ensure systems and processes are in place to monitor and evaluate risks.
- Periodically review and update the risk management policy, considering changing industry dynamics.
- Keep the Board informed about risk discussions, recommendations, and actions.
- Oversee the functioning of the Chief Risk Officer (CRO).

- Foster a risk-aware culture across the organization and integrate risk management into strategic goals.
- Conduct annual assessments of key risks and evaluate risk management processes.
- Prioritize and guide the management of critical risks at the corporate level.
- Align risk mitigation strategies with organizational objectives.
- Ensure awareness of critical risks at functional unit levels.
- Promote alignment of risk management activities across business units.
- Review reporting and management of key risks.
- Sponsor and regulate risk management initiatives.
- Review major business risks quarterly and monitor the effectiveness of risk management processes.
- Facilitate the communication of relevant risk information throughout the organization.

iii) Management:

Management ensures alignment between risk appetite and organizational goals, reviews risk strategies, and monitors the overall risk profile. They are responsible for approving mitigation plans, assigning risk owners, and overseeing risk reporting while fostering a risk-aware culture and ensuring compliance.

- Ensuring that risk management processes are integrated into decision-making.
- Establishing a culture of risk awareness across all levels of the organization.
- Reviewing and approving corrective actions for any identified gaps or deficiencies in controls.
- Ensuring compliance with regulatory requirements and internal policies related to risk.
- Overseeing the continuous improvement of risk management practices and frameworks.

iv) Chief Risk Officer:

The Chief Risk Officer (CRO) is responsible for managing the company’s risk management framework, including tracking mitigation plan progress, updating the Risk Register, and reporting on risk treatment plans (RTMs) to the Risk Management Committee. The CRO oversees the development of risk management policies, coordinates risk activities, optimizes the company’s risk portfolio, and conducts regular risk assessments and audits. The CRO ensures the implementation of mitigation strategies, monitors risk levels, and escalates critical issues to the Management Team.

- Track and report on mitigation plans and RTMs.
- Update and maintain the Risk Register.
- Coordinate risk management activities and ensure alignment with company goals.
- Develop and oversee risk management policies and processes.
- Conduct risk assessments and audits.
- Monitor and report on risk mitigation strategies and levels.
- Escalate critical risks to the Management Team.

v) Risk Owners/ Employees:

Risk Owners, typically business process owners, are responsible for managing risks, implementing controls, and ensuring mitigation plans are effective. They track risk indicators, report to the Risk Management Committee, and ensure the timely execution of action plans. The Key responsibilities are as follows:

- Identify and assess risks.
- Implement and monitor control measures and mitigation plans.
- Take ownership of risks and their management.
- Report risks and control failures with corrective actions.
- Provide regular updates to the Risk Management Committee.
- Educate employees on risk management processes.

vi) Audit Committee:

The Risk Management Committee coordinates with the Audit Committee on areas of overlap concerning audit activities.

vii) Internal Audit:

The internal auditor is responsible for conducting risk-based audits, supporting risk analysis, identifying control gaps, and advising on mitigation strategies. They provide independent assurance to the Board and Audit Committee and share best practices across the organization.

9) REVIEW OF RISK MANAGEMENT:

This risk management policy shall be reviewed as deemed necessary by the Risk Management Committee and at least once in two years, to evaluate the effectiveness of the risk management program

10) AMENDMENT

The Board of Directors of the Company shall have the power to amend any of the provisions of this Policy, substitute any of the provisions with a new provision or replace this Policy entirely with a new Policy.

Any subsequent amendment/modification in the Act or rules made thereunder or the Listing Regulations and/or other applicable laws in this regard shall automatically apply to this Policy.

*****