Risk Management Policy

[1. Purpose 2](#_Toc1839135638)

[2. Scope 3](#_Toc1939666929)

[3. Objectives 3](#_Toc281737427)

[4. Policy 3](#_Toc666482244)

[4.1 Risk Management Framework 3](#_Toc1439958491)

[4.2 Risk Appetite 3](#_Toc1425686955)

[4.3 Risk Treatment Strategies 3](#_Toc1181041372)

[4.4 Monitoring and Review 4](#_Toc1368981255)

[4.5 Reporting 4](#_Toc2025354755)

[4.6 Training and Awareness 4](#_Toc1436241142)

[4.7. Monitoring and Compliance 4](#_Toc499088105)

[5. Roles and Responsibilities 5](#_Toc903407237)

[6. Enforcement 5](#_Toc765197535)

[7. Review and Revision 5](#_Toc98206490)

[8. Document change control 5](#_Toc1548276739)

# Purpose

The purpose of this Risk Management Policy is to establish a structured and consistent approach to managing risk across the organization, enabling effective decision-making and safeguarding our assets, reputation, and operations.

# Scope

This policy applies to all employees, departments, and stakeholders involved in the organization’s activities. It covers strategic, operational, financial, legal, compliance, and reputational risks.

# Objectives

* The objectives of this policy are to:
* Identify and assess risks that could impact the organization.
* Implement risk management practices to minimize or mitigate risks.
* Ensure continuous monitoring and review of risks.
* Integrate risk management into the organizational culture and decision-making processes.

# Policy

## 4.1 Risk Management Framework

The organization adopts a risk management framework based on the following components:

* Risk Identification: Recognizing risks that may affect the organization’s objectives.
* Risk Assessment: Analyzing the likelihood and impact of identified risks.
* Risk Treatment: Developing strategies to mitigate, transfer, accept, or avoid risks.
* Monitoring and Reporting: Continuously monitoring risks and updating risk registers. Regularly reporting risks to relevant stakeholders.

## 4.2 Risk Appetite

The organization recognizes that some level of risk is inherent in its operations and seeks to manage risks within defined tolerance levels. The risk appetite is aligned with the organization’s strategic objectives and will be reviewed periodically.

## 4.3 Risk Treatment Strategies

* Avoidance: Eliminating activities that pose unacceptable risks.
* Mitigation: Reducing the likelihood or impact of risks.
* Transfer: Sharing risks with third parties (e.g., insurance).
* Acceptance: Acknowledging and accepting the risks when they fall within the risk appetite.

## 4.4 Monitoring and Review

Regular monitoring of risks is essential to ensure they remain within acceptable levels. The organization will:

* Update the risk register quarterly or as needed.
* Review and adjust the risk management framework annually.
* Conduct internal audits to assess the effectiveness of risk controls.

## 4.5 Reporting

Risk management reports will be submitted to the Board of Directors/Executive Management quarterly. The reports will include updates on the risk register, significant changes in risk status, and actions taken to address risks.

## 4.6 Training and Awareness

All employees will receive training on risk management practices and their roles in risk mitigation. The organization will promote a culture of risk awareness and proactive risk management.

## 4.7. Monitoring and Compliance

* Periodic Audits: The IT department will regularly monitor compliance with this policy through periodic audits and checks.
* Disciplinary Action: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. Contractors and third parties found in violation may have their contracts terminated.
* Training and Awareness: The IT department will provide regular training and awareness programs to ensure all employees understand the importance of this policy and their responsibilities.

# Roles and Responsibilities

* Board of Directors/Executive Management: Oversee risk management practices, review high-level risks, and set the risk appetite.
* Risk Management Committee: Develop and implement the risk management framework and policies. Conduct regular risk assessments and report to the board.
* Risk Owners: Manage specific risks assigned to them and report changes in risk levels.
* All Employees: Understand and comply with risk management practices. Report potential risks to supervisors or risk owners.
* also ensure that their own networks and systems are secure when accessing company resources.

# Enforcement

Non-compliance with this policy may lead to disciplinary action, up to and including termination of employment. Contractors and third parties found in violation may have their contracts terminated. Additionally, repeated violations may result in loss of access to company networks and systems. The company reserves the right to take legal action against individuals or entities that violate this policy and cause harm to the company’s information assets.

# Review and Revision

This policy will be reviewed annually and updated as necessary to ensure it remains effective and aligned with ISO/IEC 27001 standards. The review process will involve key stakeholders, including the IT department, management, and employee representatives.

# Document change control

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reviewed by | Reviewed Date | Reason to review | Approved by | Approved Date | Designation of the approver |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |