# ISO 27001 Risk Management Process Template

## Introduction:

This document outlines the Risk Management Process for [COMPANY NAME], aligned with ISO 27001 requirements. The process ensures that risks to the confidentiality, integrity, and availability of information assets are identified, analyzed, evaluated, treated, and monitored systematically. The Risk Management Process is an integral component of the Information Security Management System (ISMS).

## 1. Purpose of the Risk Management Process

The purpose of this process is to:  
1. Identify risks to information assets and evaluate their potential impact and likelihood.  
2. Prioritize risks based on their severity and organizational context.  
3. Implement appropriate controls to mitigate or accept risks in alignment with ISO 27001.  
4. Ensure compliance with legal, regulatory, and contractual obligations.  
5. Continuously monitor and improve risk management practices to adapt to evolving threats.

## 2. Risk Management Framework

* Context Establishment: Define scope, boundaries, stakeholders, and risk criteria.
* Risk Identification: Use tools like asset inventories, vulnerability scans, and incident analysis.
* Risk Analysis: Evaluate likelihood and impact using qualitative or quantitative methods.
* Risk Evaluation: Compare risks against criteria and prioritize for treatment.
* Risk Treatment: Select options (Mitigate, Accept, Transfer, Avoid) and document treatment plans.
* Risk Monitoring and Review: Continuously monitor risks and effectiveness of controls.
* Risk Communication: Share risk-related information with stakeholders and decision-makers.

## 3. Risk Register Template

The following table is a sample Risk Register for documenting and tracking risks:

| Risk ID | Risk Description | Likelihood | Impact | Risk Score | Treatment Plan | Status |
| --- | --- | --- | --- | --- | --- | --- |

## 4. Post-Treatment Metrics

The following metrics will be used to evaluate the success of risk treatment:

* Number of risks mitigated within a specified period.
* Reduction in risk scores after treatment.
* Number of recurring risks identified during reviews.
* Percentage of controls implemented within defined timelines.

## 5. Roles and Responsibilities

Information Security Manager (ISM):  
- Lead risk assessments and ensure appropriate treatment of risks.  
- Monitor and report on the effectiveness of risk management.

Top Management:  
- Approve risk treatment plans and provide necessary resources.  
- Ensure alignment of risk management with organizational objectives.

IT Operations Team:  
- Implement technical controls and monitor systems for emerging risks.

Compliance Officer:  
- Ensure the risk management process aligns with regulatory and contractual obligations.

Employees and Contractors:  
- Report security incidents and adhere to risk mitigation procedures.

## 6. Revision and Maintenance

This document and the Risk Management Process will be reviewed [Insert frequency, e.g., annually or as needed] to ensure it remains aligned with organizational priorities, regulatory requirements, and the threat landscape.

## Approval:

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |