## **ISO 27001 Risk Management Policy Template**

### **1. Introduction**

This document outlines the Risk Management Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes a structured approach to identifying, assessing, and mitigating risks to safeguard organizational assets and objectives.

### **2. Purpose**

The purpose of this policy is to:

1. Define a consistent framework for managing risks.
2. Protect the confidentiality, integrity, and availability of information assets.
3. Ensure compliance with ISO 27001 and other applicable regulations.
4. Promote a risk-aware culture within the organization.

### **3. Scope**

This policy applies to all employees, contractors, and third-party vendors involved in activities that could impact the organization’s information security. It encompasses:

* Physical and digital assets.
* Internal and external threats.
* Third-party risks.

### **4. Policy Statement**

[Organization Name] is committed to managing risks effectively by:

1. Conducting regular risk assessments.
2. Mitigating identified risks through appropriate controls.
3. Ensuring continuous monitoring and improvement of the risk management process.

### **5. Risk Management Framework**

#### **5.1 Risk Identification**

1. Identify potential threats, vulnerabilities, and impacts on organizational assets.
2. Use tools such as interviews, audits, and threat modeling for comprehensive risk identification.
3. Document risks in the organization’s risk register.

#### **5.2 Risk Assessment**

1. Assess risks based on their likelihood and impact.
2. Assign risk levels (e.g., low, medium, high, critical).
3. Prioritize risks for mitigation based on their assessed level.

#### **5.3 Risk Treatment**

1. Determine appropriate risk treatment strategies:
   * Mitigate: Apply controls to reduce risk.
   * Transfer: Share risk with a third party (e.g., insurance).
   * Accept: Acknowledge and monitor the risk without further action.
   * Avoid: Eliminate the activity causing the risk.
2. Implement and document mitigation plans.

#### **5.4 Risk Monitoring and Review**

1. Monitor risks and their treatment plans regularly.
2. Update the risk register as new risks emerge or existing risks change.
3. Conduct periodic reviews to ensure the effectiveness of risk management activities.

### **6. Roles and Responsibilities**

1. **Risk Owners:** Identify and assess risks within their areas and ensure mitigation actions are implemented.
2. **Risk Management Team:** Facilitate risk assessments, maintain the risk register, and support mitigation efforts.
3. **Information Security Officer (ISO):** Oversee the risk management process and ensure compliance with ISO 27001 requirements.
4. **Executive Leadership:** Review and approve risk treatment strategies and decisions for high-priority risks.

### **7. Compliance and Monitoring**

1. Conduct regular audits to ensure adherence to this policy and ISO 27001 standards.
2. Monitor for emerging risks and adjust controls accordingly.
3. Address non-compliance through corrective actions or disciplinary measures.

### **8. Related Documentation**

1. Information Security Policy
2. Incident Management Policy
3. Business Continuity Plan

### **9. Review and Revision**

This policy will be reviewed annually or whenever significant changes occur in the organization’s risk landscape or regulatory requirements. Updates will be approved by the Information Security Officer.

### **Appendix A: Risk Register Template**

| **Risk ID** | **Description** | **Likelihood** | **Impact** | **Risk Level** | **Treatment Strategy** | **Owner** | **Status** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

### **Appendix B: Risk Assessment Checklist**

| Assessment Area | Question | Response | Notes |
| --- | --- | --- | --- |
|  |  |  |  |

### **Appendix C: Policy Acknowledgment Form**

I acknowledge that I have read and understood the Risk Management Policy and agree to comply with its requirements.

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_