Heimdal®

Cybersecurity Risk Management Template

Effective cybersecurity risk management is not just a technical necessity but a strategic imperative for businesses of all sizes and sectors. Recognizing this critical need, we have developed a comprehensive Cybersecurity Risk Management Template to guide organizations through the process of identifying, assessing, and mitigating cybersecurity risks.

This template is designed to be adaptable, providing a structured approach that organizations can customize to fit their unique needs and risk profiles.

1. Document Control

Document Information	Details
Title	Cybersecurity Risk Management Template
Date	[Date]
Version	[Version]
Author	[Author's Name]
Approval	[Approver's Name]

Purpose

Define the purpose of the cybersecurity risk management plan. This could include protecting organizational assets, ensuring data integrity, and compliance with regulations.

Scope

Detail the scope of the plan, specifying the parts of the organization it covers, such as systems, data, and processes.

Responsibilities

List roles and responsibilities for cybersecurity within the organization, including risk management teams, IT staff, and other stakeholders.

2. Risk Identification & Analysis

Risk ID	Description	Source	Likelihood	Impact (Low, Medium, High)	Priority
				Low	

3. Risk Mitigation Strategies

Risk ID	Mitigation Strategy	Preventive Measures	Detection Measures	Response Strategies	Recovery Plans

4. Implementation Plan

Action Item ID	Strategy	Responsible Party	Deadline	Status	Notes
				Not Sta…	

5. Training and Awareness Plan

Program ID	Program Type	Target Audience	Frequency	Responsible Party	Status
					Not Sta…

6. Monitoring and Review Schedule

Activity ID	Activity Type	Frequency	Responsible Party	Last Review Date	Next Review Date

7. Compliance and Reporting

Requirement ID	Regulation / Standard	Compliance Measures	Reporting Protocol	Responsible Party	Compliance Status
					Not Sta…

8. Review and Approval

The cybersecurity risk management has identified several areas requiring immediate attention, notably in data protection, access controls, and employee training. The management also highlighted the organization's strengths, such as a robust incident response plan and effective use of encryption technologies.

Going forward, it is recommended that the organization:

- Enhances data protection measures by implementing stricter access controls and regular audits.
- Increases employee cybersecurity awareness training to reduce the risk of phishing and social engineering attacks.
- Strengthens network security through the adoption of next-generation firewalls and intrusion detection systems.
- Reviews and updates the incident response plan to address emerging threats.

Approval

- **[Text Field for Approver Name]**
- **[Signature Field]**
- **[Date]**