## 

## Cybersecurity Risk Assessment Template

**Organization Name:** [Text Field]

**Assessment Date:** [Date]

**Next Review Date:** [Date]

### Section 1: Assessment Overview

#### Purpose of Assessment

| **Compliance** | **Incident Response Planning** | **Information Security Program Development** | **Other (Please Specify)** |
| --- | --- | --- | --- |
| **✅** | **✅** | **✅** | **✅** |

#### Scope of Assessment

The cybersecurity risk assessment covers all critical IT infrastructure, applications, and data handled by our organization across all departments and locations. This includes, but is not limited to, network infrastructure, servers, workstations, mobile devices, cloud services, and third-party services. The assessment aims to identify potential vulnerabilities and threats, assess the likelihood and impact of these threats, and recommend appropriate mitigation strategies to ensure the confidentiality, integrity, and availability of organizational data.

#### Assessment Team

| **Name** | **Role** | **Department** | **Contact Information** |
| --- | --- | --- | --- |
|  |  |  |  |

Methodology

Our cybersecurity risk assessment methodology is based on industry best practices and standards, including the NIST Cybersecurity Framework and ISO/IEC 27001.

### Section 2: Asset Inventory

#### Assets Identification

| **Asset ID** | **Asset Name** | **Asset Type** | **Owner** | **Location** | **Criticality (Low, Medium, High)** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | Low |

### Section 3: Threat Identification

#### Threat Sources

| **External (Cybercriminals, Hacktivists)** | ✅ |
| --- | --- |
| **Internal (Employees, Contractors)** | ✅ |
| **Third-Party (Vendors, Partners)** | ✅ |

#### Threat Types

| **Malware** | ✅ |
| --- | --- |
| **Phishing** | ✅ |
| **DDoS** | ✅ |
| **Insider Threat** | ✅ |
| **Ransomware** | ✅ |

### Section 4: Vulnerability Identification

#### Vulnerabilities Listing

| **Vulnerability ID** | **Description** | **Asset Affected** | **Source (External/Internal)** | **Detection Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

### Section 5: Risk Analysis

#### Risk Evaluation

| **Risk ID** | **Threat** | **Vulnerability** | **Impact (Low, Medium, High)** | **Likelihood (Low, Medium, High)** | **Risk Level (Auto-calculated)** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | Low | Low |

### Mitigation Actions

| **Action ID** | **Description** | **Responsible Party** | **Deadline** | **Status (Not Started, In Progress, Completed)** |
| --- | --- | --- | --- | --- |
|  |  |  |  | Not Started |

### Section 7: Review and Approval

#### Assessment Review:

#### The cybersecurity risk assessment has identified several areas requiring immediate attention, notably in data protection, access controls, and employee training. The assessment 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]**