Cybersecurity Risk Assessment Report

Organization Name:
Assessment Date: [Insert Date]
Next Review Date: [Insert Next Review Date]

Section 1: Assessment Overview

Purpose of Assessment

☑ Compliance
☑ Incident Response Planning
☑ Information Security Program Development
☑ Other: Security Control Gap Analysis

Scope of Assessment

This cybersecurity risk assessment evaluates critical IT infrastructure, applications, and data across all departments and locations. The assessment covers:

- Network Infrastructure: Servers, workstations, routers, and wireless networks.
- Cloud Services & Third-Party Integrations: Email systems, data storage, vendor platforms.
- End-User Devices: Laptops, desktops, and mobile devices.
- Physical Security: Access controls to IT infrastructure, server rooms, and data centers.

The goal is to identify vulnerabilities, assess risks, and recommend mitigation strategies to ensure the confidentiality, integrity, and availability (CIA) of organizational data.

Assessment Team

Name	Role	Department	Contact Information
[Your Name]	IT Security Lead	IT Department	[Your Contact]
[Other Team Member]	Compliance Officer	Risk Management	[Contact]
[Other Team Member]	Incident Response Manager	SOC	[Contact]

Methodology

This assessment follows industry best practices and NIST 800-53 standards, using a risk-based approach to:

- Identify threats and vulnerabilities.
- Evaluate risk likelihood and impact.

- Develop actionable mitigation strategies.

Section 2: Asset Inventory

Asset ID	Asset Name	Asset Type	Owner	Location	Criticality (Low, Medium, High)
A001	Main Server	Hardware	IT Dept.	Data Center	High
A002	Employee Workstations	Hardware	All Employees	Office	Medium
A003	Email System	Cloud Service	IT Dept.	Microsoft Cloud	High
A004	Internal Database	Software	IT Dept.	Data Center	High
A005	Firewall & Network Devices	Hardware	Network Admin	IT Room	High
A006	Customer Database	Database	IT Security	Secure Server	High

Section 3: Threat Identification

Threat Sources

☑ External (Cyber-related, Physical, Terrain)
☑ Internal (Employees, Contractors, Third Parties)
☑ Third-Party (Vendors, Applications, Cloud Providers)

Threat Types

☑ Malware/Ransomware
☑ Phishing
☑ DDoS Attacks
☑ Insider Threat
☑ Theft
☑ Social Engineering

Section 4: Vulnerability Identification

Vulnerability ID	Description	Asset Affected	Source (External/Internal)	Detection Date
V001	No Penetration Testing	Main Server	Internal	2025-01-29
V002	Unsegmented Network	Entire Network	Internal	2025-01-29
V003	Weak Email Security	Email System	External	2025-01-29
V004	No Documented Incident Response Plan	Entire Organization	Internal	2025-01-29
V005	Weak Physical Security	Server Room	Internal	2025-01-29
V006	No Multi-Factor Authentication (MFA)	Email System, Database	Internal	2025-01-29
V007	Outdated Security Patches on Workstations	Workstations	Internal	2025-01-29
V008	Misconfigured Cloud Access Controls	Cloud Services	External	2025-01-29

Section 5: Risk Analysis

Risk ID	Threat	Vulnerability	Impact (Low, Medium, High)	Likelihood (Low, Medium, High)	Risk Level
R001	Data Breach	No MFA on Critical Systems	High	High	Critical
R002	Unauthorized Access	No RBAC Implementation	High	Medium	High
R003	Ransomware Attack	Unsegmented Network	High	High	Critical
R004	Phishing Attacks	Weak Email Security (No DMARC, SPF, DKIM)	Medium	High	High

R005	Physical Theft	Weak Physical Security (Unsecured Server Room)	High	Medium	High
R006	Insider Threat	Lack of User Activity Monitoring	High	Medium	High
R007	DDoS Attack	No Network Traffic Filtering	Medium	High	High
R008	Data Integrity Failure	No Regular Data Backups	High	Medium	High
R009	Third-Party Risk	Unverified Vendor Security Controls	Medium	Medium	Medium
R010	Unpatched Systems	No Regular Vulnerability Patching	High	High	Critical

Section 6: Mitigation Actions

Action ID	Description	Responsible Party	Deadline	Status (Not Started, In Progress, Completed)
M001	Conduct Penetration Testing	IT Security	2025-03-15	Not Started
M002	Implement Network Segmentation	Network Admin	2025-04-01	In Progress
M003	Enable Email Security Protections (DMARC, SPF, DKIM)	IT Security	2025-02-20	Not Started
M004	Implement Multi-Factor Authentication (MFA)	Compliance Team	2025-03-01	Not Started
M005	Secure Physical Access to Server Room	Facilities Management	2025-03-10	In Progress

Action ID	Description	Responsible Party	Deadline	Status (Not Started, In Progress, Completed)
M006	Develop and Document Incident Response Plan	IT & Security Teams	2025-04-15	Not Started
M007	Conduct Regular Security Awareness Training	Compliance Team	2025-03-01	Not Started

SMART Goal:

"By July 29, 2025, will implement multi-factor authentication (MFA), role-based access control (RBAC), network segmentation, email security protections (DMARC, SPF, DKIM), and a documented Incident Response Plan (IRP). Success will be measured by compliance with NIST 800-53 standards and a reduction in identified vulnerabilities."

Section 7: Implementation Timeline (6-Month Plan)

Milestone	Action Items	Responsible Party	Deadline
Month 1	Security audit, finalize risk assessment.	IT Security Team	February 28, 2025
Month 2	Deploy Multi-Factor Authentication (MFA).	IT Security Team	March 29, 2025
Month 3	Implement Role-Based Access Control (RBAC).	Compliance Team	April 29, 2025
Month 4	Enable Email Security Protections.	Security Awareness Team	May 29, 2025
Month 5	Complete Network Segmentation.	Network Admins	June 29, 2025
Month 6	Finalize and test Incident Response Plan (IRP). Conduct penetration testing.	IT & Incident Response Teams	July 29, 2025

Section 8: Review & Approval

Assessment Review

The cybersecurity risk assessment identified key areas requiring immediate attention, including:

- Strengthening access control measures (MFA, RBAC).
- Enhancing email security protections to prevent phishing attacks.
- Implementing network segmentation to reduce lateral movement risks.
- Securing physical access to critical IT assets.
- Developing a formalized Incident Response Plan (IRP).

A structured six-month roadmap has been established to address these vulnerabilities and align with NIST 800-53 standards.

Recommendations:

- Enhance security by deploying MFA and RBAC within three months.
- Increase monitoring by implementing email security protocols (DMARC, SPF, DKIM) within four months.
- Review and update network segmentation and fully deploy an IRP within six months.

Approval

Approver Name	Signature	Date
[Name]	[Signature]	[Date]