Rick Abraham

My Company  Dallas, TX

Risk Assessment – Third-Party Risks

Contents

[Introduction 2](#_Toc182582686)

[Purpose 2](#_Toc182582687)

[Scope 2](#_Toc182582688)

[Risk Identification 2](#_Toc182582689)

[Risk Analysis 3](#_Toc182582690)

[Mitigation Recommendations 3](#_Toc182582691)

[Sensitive Data 3](#_Toc182582692)

[Network Infrastructure 3](#_Toc182582693)

[Supply Chain Operations 4](#_Toc182582694)

[Compliance Requirements 4](#_Toc182582695)

[Vendor Management Accounts 4](#_Toc182582696)

[Monitoring and Review 4](#_Toc182582697)

[Frequency 4](#_Toc182582698)

[Daily 4](#_Toc182582699)

[Monthly 4](#_Toc182582700)

[Quarterly 5](#_Toc182582701)

[Bi-Annually 5](#_Toc182582702)

[Annually 5](#_Toc182582703)

[Incident Response 5](#_Toc182582704)

[Documentation and Compliance 5](#_Toc182582705)

Risk Assessment – Third-Party Risks

# Introduction

Purpose: This risk assessment identifies and evaluates potential risks introduced by third-party vendors, contractors, and partners. It outlines vulnerabilities in vendor access, compliance gaps, and weak security practices, providing recommendations to mitigate these risks.

Scope: Includes third-party access to systems, data, and physical facilities, as well as outsourced services such as cloud hosting, managed IT services, and supply chain processes.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Sensitive Data | Unauthorized access by vendor personnel | Inadequate access controls or monitoring | Data breaches, regulatory penalties | High |
| Network Infrastructure | Malware introduced through third-party integrations | Lack of security vetting or monitoring of vendor software | System compromise, operational disruption | High |
| Supply Chain Operations | Disruption caused by vendor system outages | Dependency on vendor infrastructure | Downtime, reputational damage | Medium |
| Compliance Requirements | Non-compliance by vendors impacting the organization | Inadequate vendor due diligence | Legal and financial penalties | Medium |
| Vendor Management Accounts | Exploitation of vendor accounts for lateral movement | Weak authentication and monitoring of vendor activity | Unauthorized access, data exfiltration | High |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Sensitive Data | Medium | High | High |
| Network Infrastructure | High | High | Critical |
| Supply Chain Operations | Medium | Medium | Moderate |
| Compliance Requirements | Medium | Medium | Moderate |
| Vendor Management Accounts | High | High | Critical |

# Mitigation Recommendations

## Sensitive Data

* Enforce **least-privilege principles** for vendor access to sensitive data.
* Require all vendors to comply with data protection standards, such as **GDPR** or **CCPA**.
* Implement **Data Loss Prevention (DLP)** tools to monitor and block unauthorized data transfers by third-party users.

## Network Infrastructure

* Vet vendor-provided software for malware and vulnerabilities before deployment.
* Segregate vendor access to specific network zones using **network segmentation**.
* Continuously monitor third-party integrations for anomalous activity using **Intrusion Detection/Prevention Systems (IDS/IPS)**.

## Supply Chain Operations

* Maintain backup vendor agreements to reduce reliance on a single provider.
* Monitor vendor performance and establish Service Level Agreements (SLAs) with strict uptime requirements.
* Regularly review supply chain security practices to identify potential weaknesses.

## Compliance Requirements

* Conduct **vendor risk assessments** before onboarding and annually to ensure ongoing compliance with applicable regulations.
* Include data security and compliance clauses in vendor contracts, with penalties for breaches or non-compliance.
* Require vendors to provide regular compliance reports and participate in external audits.

## Vendor Management Accounts

* Enforce **multi-factor authentication (MFA)** for all vendor accounts accessing organizational systems.
* Monitor vendor account activity logs for unusual behavior, such as large data transfers or logins from unexpected locations.
* Disable vendor accounts immediately after contract termination or inactivity.

# Monitoring and Review

Frequency

### Daily

* Monitor vendor access logs for unusual activities, including unauthorized data transfers or anomalous login patterns.
* Validate alerts from IDS/IPS systems for suspicious activity related to third-party connections.

### Monthly

* Review vendor access permissions and adjust based on current project needs or contract status.
* Audit vendor-provided software and integrations for performance and security vulnerabilities.
* Ensure third-party SLA compliance by reviewing up-time reports and incident resolution times.

### Quarterly

* Conduct third-party risk assessments to evaluate the security posture of vendors.
* Review compliance certifications provided by vendors, ensuring they meet regulatory requirements.
* Audit vendor contracts for data protection clauses and alignment with organizational policies.

### Bi-Annually

* Perform penetration testing on third-party integrations to uncover potential vulnerabilities.
* Conduct tabletop exercises simulating vendor-related incidents, such as a third-party system compromise.
* Evaluate vendor business continuity plans to ensure minimal disruption in case of outages or attacks.

### Annually

* Reassess third-party risks in light of changes to vendor services, organizational infrastructure, or regulatory environments.
* Update vendor onboarding and risk assessment processes to incorporate lessons learned from incidents and audits.
* Conduct an organization-wide vendor security awareness campaign to reinforce best practices for managing third-party access.

Incident Response

* Establish a Third-Party Incident Response Team (TPIRT) to address and resolve vendor-related security breaches.
* Conduct bi-annual incident response drills, focusing on scenarios such as vendor account compromises or third-party malware outbreaks.
* Document all third-party security incidents, including root causes, remediation steps, and lessons learned.

Documentation and Compliance

* Maintain logs of third-party access activities, including data transfers, software deployments, and account usage.
* Document vendor onboarding processes, risk assessments, and compliance certifications.
* Ensure compliance with applicable standards, including:
  + NIST SP 800-53: SA-9 (External System Services), AC-17 (Remote Access), and SI-4 (Monitoring).
  + GDPR, ISO 27001, and SOC 2 requirements for third-party management.