##

## **Vendor Risk Assessment Template**

### **Purpose**

The purpose of this Vendor Risk Assessment Template is to provide organizations with a structured, systematic approach to evaluating the risks associated with engaging third-party vendors.

By leveraging this template, businesses can:

1. Identify potential security, operational, financial, and compliance risks introduced by vendors.
2. Ensure that vendors meet the organization's standards for data protection, reliability, and regulatory compliance.
3. Mitigate the likelihood of supply chain vulnerabilities, data breaches, or disruptions to critical operations.
4. Foster informed decision-making regarding vendor selection, approval, and monitoring.

### **Scope**

This Vendor Risk Assessment Template applies to any vendor, supplier, or third-party service provider that interacts with the organization, including but not limited to:

* IT service providers (e.g., cloud services, SaaS platforms, IT infrastructure providers).
* Software vendors and developers.
* Consultants and contractors handling sensitive or critical operations.
* Suppliers in the production or supply chain.
* Any third party with access to the organization’s systems, networks, or data.

### **1. General Information**

| **Section** | **Details to Fill In** |
| --- | --- |
| **Vendor Name:** |  |
| **Contact Person:** |  |
| **Vendor Website/Address:** |  |
| **Service/Product Provided:** |  |
| **Assessment Date:** |  |
| **Assessed By (Your Team)** |  |

### **2. Criticality Assessment**

Evaluate how critical this vendor is to your operations.

| **Category** | **Questions** | **Response (High/Medium/Low)** | **Comments** |
| --- | --- | --- | --- |
| **Operational Dependency** | How essential is this vendor to daily operations? |  |  |
| **Financial Impact** | Would disruption significantly impact revenue? |  |  |
| **Data Sensitivity** | Do they handle sensitive/confidential data? |  |  |
| **Volume of Interaction** | How frequently do you interact with this vendor? |  |  |

### **3. Vendor Security Practices**

Assess the vendor’s cybersecurity practices and their approach to risk management.

| **Security Practice** | **Questions** | **Yes/No** | **Comments/Evidence** |
| --- | --- | --- | --- |
| **Security Policies** | Does the vendor have documented security policies? |  |  |
| **Third-Party Certifications** | Do they hold certifications (ISO 27001, SOC 2, etc.)? |  | List certifications if any. |
| **Data Protection Measures** | Is data encrypted (in transit and at rest)? |  |  |
| **Incident Response Plan** | Do they have an incident response procedure? |  |  |
| **Access Controls** | Are role-based access controls (RBAC) implemented? |  |  |
| **Vulnerability Management** | How frequently do they perform vulnerability scans? |  |  |
| **Employee Training** | Do employees undergo cybersecurity training? |  |  |
| **Penetration Testing** | Is regular penetration testing conducted? |  |  |
| **Backup and Recovery** | Do they have data backup and recovery plans? |  |  |

### **4. Compliance and Legal Requirements**

Determine if the vendor meets regulatory and legal compliance needs.

| **Compliance Area** | **Questions** | **Yes/No** | **Details/Evidence** |
| --- | --- | --- | --- |
| **GDPR/CCPA Compliance** | Do they comply with relevant data protection laws? |  |  |
| **Industry Standards** | Are they compliant with relevant industry regulations? |  | E.g., HIPAA, PCI DSS |
| **Contracts and SLAs** | Are agreements and SLAs up-to-date and in place? |  |  |
| **Audit Rights** | Can you audit their practices if needed? |  |  |

###

### **5. Financial Stability**

Ensure the vendor’s financial health to assess long-term reliability.

| **Financial Assessment Area** | **Questions** | **Yes/No** | **Details** |
| --- | --- | --- | --- |
| **Financial Statements** | Can they provide recent financial statements? |  | Attach or comment. |
| **Years in Business** | How long has the vendor been in operation? |  |  |
| **Financial Risk** | Are there any risks of bankruptcy? |  | Research or ask the vendor. |

### **6. Performance and Reliability**

Evaluate the vendor’s ability to meet expectations.

| **Performance Metric** | **Questions** | **Response** | **Comments** |
| --- | --- | --- | --- |
| **Service Uptime** | What is their average uptime SLA (e.g., 99%)? |  |  |
| **Support Availability** | Do they provide 24/7 customer support? |  |  |
| **Resolution Time** | What is their average issue resolution time? |  |  |
| **Past Performance** | Are there records of past incidents/failures? |  |  |

### **7. Risk Scoring Summary**

Summarize the risks identified from the above sections.

| **Risk Category** | **Risk Level (High/Medium/Low)** | **Comments** |
| --- | --- | --- |
| **Operational Risk** |  |  |
| **Compliance Risk** |  |  |
| **Cybersecurity Risk** |  |  |
| **Financial Risk** |  |  |
| **Performance Risk** |  |  |

### **8. Final Recommendation**

| **Overall Risk Level** (High/Medium/Low): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

### **9. Vendor Risk Assessment Checklist (Quick Recap)**

| **Item** | **Completed? (Yes/No)** | **Comments** |
| --- | --- | --- |
| Vendor Information Collected |  |  |
| Criticality Assessment Completed |  |  |
| Security Practices Evaluated |  |  |
| Compliance Requirements Reviewed |  |  |
| Financial Stability Checked |  |  |
| Performance and Reliability Assessed |  |  |
| Risk Levels Scored and Summarized |  |  |
| Risk Levels Scored and Summarized |  |  |