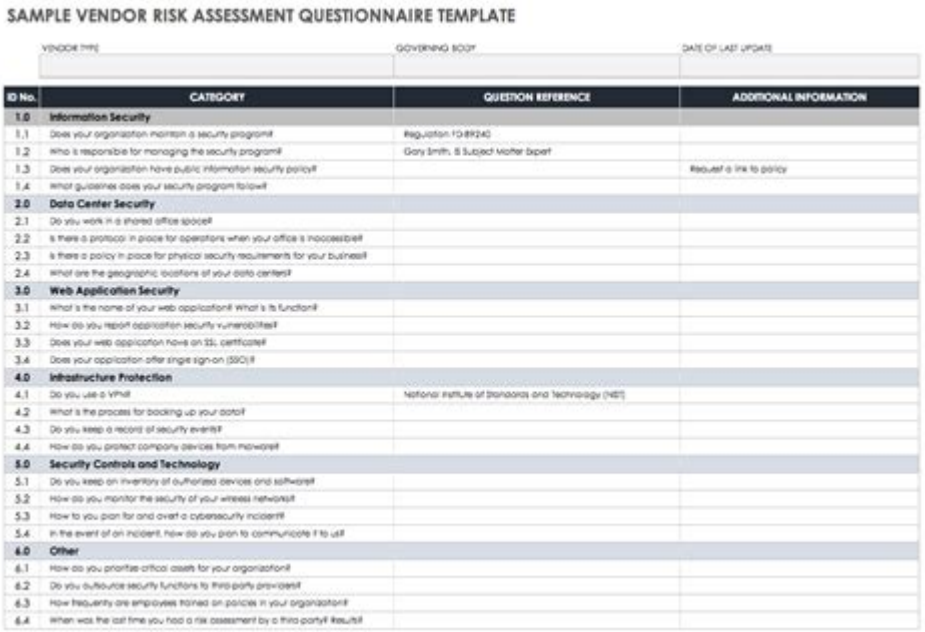
# Nist Vendor Risk Assessment Questionnaire



SAMPLE VENDOR RISK ASSESSMENT QUESTIONNAIRE TEMPLATE

| VENDOR TYPE | GOVERNING BODY | DATE OF LAST UPDATE |
|---|---|---|
| | | |

| ID No. | CATEGORY | QUESTION REFERENCE | ADDITIONAL INFORMATION |
|---|---|---|---|
| 1.0 | **Information Security** | | |
| 1.1 | Does your organization maintain a security program? | Regulation 10 CFR 240 | |
| 1.2 | Who is responsible for managing the security program? | Gary Smith, IS Subject Matter Expert | |
| 1.3 | Does your organization have public information security policy? | | Request a link to policy |
| 1.4 | What guidelines does your security program follow? | | |
| 2.0 | **Data Center Security** | | |
| 2.1 | Do you work in a shared office space? | | |
| 2.2 | Is there a protocol in place for operations when your office is inaccessible? | | |
| 2.3 | Is there a policy in place for physical security requirements for your business? | | |
| 2.4 | What are the geographic locations of your data centers? | | |
| 3.0 | **Web Application Security** | | |
| 3.1 | What is the name of your web application? What is its function? | | |
| 3.2 | How do you report application security vulnerabilities? | | |
| 3.3 | Does your web application have an SSL certificate? | | |
| 3.4 | Does your application offer single sign-on (SSO)? | | |
| 4.0 | **Infrastructure Protection** | | |
| 4.1 | Do you use a VPN? | National Institute of Standards and Technology (NIST) | |
| 4.2 | What is the process for backing up your data? | | |
| 4.3 | Do you keep a record of security events? | | |
| 4.4 | How do you protect company devices from malware? | | |
| 5.0 | **Security Controls and Technology** | | |
| 5.1 | Do you keep an inventory of authorized devices and software? | | |
| 5.2 | How do you monitor the security of your wireless networks? | | |
| 5.3 | How to you plan for and avert a cybersecurity incident? | | |
| 5.4 | In the event of an incident, how do you plan to communicate it to us? | | |
| 6.0 | **Other** | | |
| 6.1 | How do you prioritize critical assets for your organization? | | |
| 6.2 | Do you outsource security functions to third-party providers? | | |
| 6.3 | How frequently are employees trained on policies in your organization? | | |
| 6.4 | When was the last time you had a risk assessment by a third-party? Results? | | |

**NIST Vendor Risk Assessment Questionnaire** is an essential tool designed to help organizations assess the security and risk posture of their third-party vendors. With the growing reliance on external suppliers and service providers, understanding the risks they introduce has become a critical aspect of maintaining robust cybersecurity standards. The National Institute of Standards and Technology (NIST) provides guidelines and frameworks that help organizations identify and mitigate these risks effectively. This article delves into the importance of the NIST Vendor Risk Assessment Questionnaire, its structure, and how organizations can implement it to enhance their risk management practices.

## The Importance of Vendor Risk Management

Vendor risk management (VRM) is crucial for organizations that work with third parties. As businesses become increasingly interconnected, the potential for risks posed by vendors has escalated. Here are several reasons why effective VRM is essential:

1. Data Protection: Vendors often handle sensitive data, and any breach can have catastrophic consequences for an organization.
2. Regulatory Compliance: Many industries are governed by strict regulations regarding data security. Failing to manage vendor risks can result in non-compliance and hefty fines.
3. Business Continuity: Disruptions in vendor services can affect an organization’s ability to operate. Understanding vendor risks helps ensure business continuity.
4. Reputation Management: A security incident involving a vendor can damage an organization’s reputation, leading to loss of customer trust and business opportunities.

# NIST Guidelines and Standards

NIST has developed a variety of guidelines and standards that facilitate effective risk management, including the NIST Cybersecurity Framework (CSF) and Special Publications (SP). The NIST Vendor Risk Assessment Questionnaire is aligned with these standards and enables organizations to evaluate vendor security practices comprehensively.