VENDOR RISK MANAGEMENT CHECKLIST

PROTECT YOUR ORGANIZATION FROM CYBER THREATS, DATA BREACHES, AND COMPLIANCE FAILURES

Managing third-party vendor risk is no longer optional. With the rise of data breaches, ransomware, and evolving compliance requirements, organizations must be vigilant about who they partner with and how data is shared. This checklist will help you assess, manage, and monitor vendor risk using best practices aligned with **SOC 1, SOC 2, and NIST Cybersecurity Frameworks.**

1. VENDOR PRE-SCREENING

Before engaging with any third-party vendor, evaluate their security posture and risk exposure.

- [ ] Do they have current SOC 1 or SOC 2 reports (Type I or Type II)?
- [ ] Are they compliant with any applicable NIST standards (e.g., NIST 800-53 or NIST CSF)?
- [ ] Can they provide recent penetration test results or security assessments?
- [ ] Are their data handling and storage practices clearly documented?
- [ ] Do they use subcontractors, and if so, are those vendors also assessed?

2. DUE DILLIGENCE & RISK ASSESSMENT

Assess the vendor's security practices based on the sensitivity of the services/data involved.

- [ ] Have you completed a vendor risk assessment questionnaire?
- [ ] Is the vendor categorized by risk level (Low, Medium, High)?
- [ ] Does the vendor have a formal risk management program?
- [ ] Have you evaluated their data breach history?
- [ ] Are their security controls aligned with your industry's regulatory requirements (i.e., HIPAA, GLBA, PCI DSS)?

CONTACT US

614.407.7990 sales@3sgplus.com www.3sgplus.com

VENDOR RISK MANAGEMENT CHECKLIST

3. CONTRACTUAL SAFEGUARDS

Ensure legal agreements reflect your organization's risk appetite and security requirements.

- [ ] Does the contract include specific language on data protection, privacy, and breach notification?
- [ ] Are security requirements and service level agreements (SLAs) clearly defined?
- [ ] Is the vendor required to notify your organization within a specific time if a breach occurs?
- [ ] Does the agreement include rights to audit or require annual compliance verification?

4. ONGOING MONITORING & AUDITING

Security isn't one-and-done. Continuous oversight helps catch issues early.

- [ ] Is there a schedule for periodic vendor risk reviews?
- [ ] Do you monitor for changes in SOC report status, certifications, or financial health?
- [ ] Are there KPIs or compliance metrics defined and tracked?
- [ ] Is there a documented process for escalation in the event of non-compliance?

5. INCIDENT RESPONSE COORDINATION

Make sure the vendor is prepared—and that your teams are in sync.

- [ ] Does the vendor have an Incident Response (IR) Plan?
- [ ] Are roles and responsibilities defined in a joint response scenario?
- [ ] Do you conduct tabletop exercises or drills with key vendors?
- [ ] Are communication protocols defined for cyber incidents?

CONTACT US

614.407.7990 sales@3sgplus.com www.3sgplus.com

VENDOR RISK MANAGEMENT CHECKLIST

6. END OF CONTRACT PROCEDURES

When the relationship ends, security must still be maintained.

- [ ] Is there a documented offboarding process?
- [ ] Are all access points and credentials revoked immediately?
- [ ] Is data return or destruction confirmed and documented?
- [ ] Is a final compliance review conducted?

BONUS: BEST PRACTICE ALIGNMENT

To align with SOC 2 (Trust Services Criteria) and NIST CSF, prioritize these best practices:

- [x] Encrypt data in transit and at rest.
- [x] Enforce strong access controls (i.e., least privilege, MFA).
- [x] Maintain up-to-date inventories of all vendors and systems they access.
- [x] Use centralized logging and monitoring for vendor activity.
- [x] Document and test Business Continuity and Disaster Recovery plans.

FINAL TIP

Vendor risk isn't just an IT problem—it's a business risk. Align your procurement, legal, and compliance teams to ensure comprehensive oversight.

NEED HELP GETTING STARTED?

3SG Plus provides Governance, Risk, and Compliance (GRC) audit services tailored to help organizations assess vendor risk, achieve SOC 1/SOC 2 readiness, and align with NIST standards.

Let us help you build a stronger, more secure vendor ecosystem. Contact us today to schedule a GRC audit or learn how our team can support your vendor risk management strategy.

CONTACT US

614.407.7990 sales@3sgplus.com www.3sgplus.com