Third Party Risk Management Guide

A comprehensive framework for managing vendor and third-party security risks in your organization. Developed by the Cybersecurity Non-Profit to help small and medium businesses protect their data and operations.

FOUNDATION

Understanding Third Party Risk

Third party risk refers to potential security threats and vulnerabilities introduced when you share data or grant system access to external vendors, suppliers, or service providers. Every vendor relationship creates a potential entry point for cyber threats.

Why This Matters

- 60% of data breaches involve third parties
- Vendor access can bypass your security controls
- Regulatory compliance requires vendor oversight
- Reputation damage extends beyond your organization

Key Risk Categories

Data Security: Unauthorized access or data breaches

Operational: Service disruptions or failures

Compliance: Regulatory violations through vendors

Reputational: Association with compromised partners

STEP 1

Vendor Categorization Framework

Not all vendors pose equal risk. Categorize your vendors based on data access, system privileges, and business criticality to focus your risk management efforts effectively.

Critical Risk

Access Level: Full system access or handles sensitive data

Examples: Cloud service providers, payroll processors, IT managed services

Assessment: Comprehensive annual reviews with continuous monitoring

High Risk

Access Level: Limited system access or handles confidential information

Examples: CRM platforms, email providers, customer support tools

Assessment: Detailed reviews every 12-18 months

Medium Risk

Access Level: Restricted access to non-sensitive data

Examples: Marketing tools, office suppliers with limited portal access

Assessment: Standard reviews every 2-3 years

Low Risk

Access Level: No system access or data handling

Examples: Physical suppliers, landscaping services, catering

Assessment: Basic verification and periodic spot checks

STEP 2

Due Diligence Process

Conduct thorough vendor assessments before engagement to identify potential risks and security gaps. This proactive approach prevents costly security incidents down the road.

01

Initial Screening

Review vendor security documentation, certifications (ISO 27001, SOC 2), and public reputation. Check for past security incidents or compliance violations.

02

Security Questionnaire

Distribute standardized security assessment covering data protection practices, access controls, encryption standards, incident response capabilities, and backup procedures.

03

Documentation Review

Examine security policies, privacy notices, business continuity plans, and insurance coverage. Verify compliance with relevant regulations (GDPR, HIPAA, PCI-DSS).

04

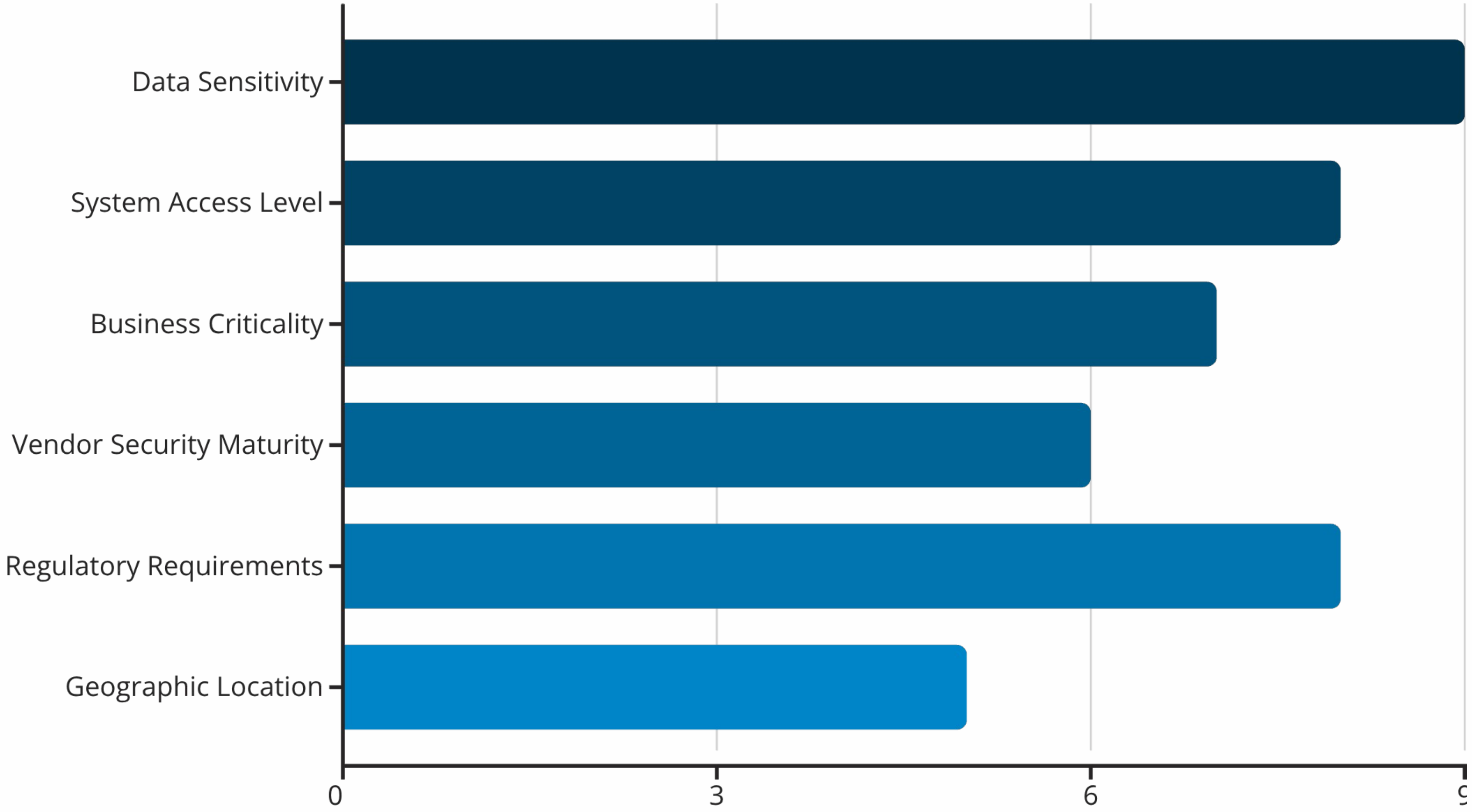
Risk Evaluation

Analyze findings against your risk tolerance. Identify gaps, request remediation plans, and determine if risks are acceptable or require additional controls before proceeding.

STEP 3

Risk Assessment Framework

Evaluate vendor risk systematically using a standardized matrix. This framework helps prioritize resources and make informed decisions about vendor relationships and required security controls.



Risk Scoring

8-10: Critical - Immediate action required

5-7: High - Priority mitigation needed

3-4: Medium - Monitor and improve

1-2: Low - Standard controls sufficient

Assessment Frequency

- Critical vendors: Quarterly reviews
- High-risk vendors: Semi-annual reviews
- Medium-risk: Annual assessments
- Low-risk: Every 2-3 years or as needed

STEP 4

Contract Security Requirements

Strong contractual protections are your legal foundation for vendor security. Ensure every vendor agreement includes comprehensive security clauses that define expectations, responsibilities, and consequences.

Data Protection Clauses

- Specify data ownership and usage rights
- Require encryption in transit and at rest
- Define data retention and deletion procedures
- Include data localization requirements if applicable

Security Standards

- Mandate specific security certifications
- Require multi-factor authentication (MFA)
- Define acceptable access control measures
- Specify vulnerability management timelines

Audit Rights

- Reserve right to conduct security audits
- Request SOC 2 or similar reports annually
- Include on-site inspection capabilities
- Define audit notification requirements

Incident Response

- Establish breach notification timelines (24-72 hours)
- Define incident investigation cooperation
- Specify liability and indemnification terms
- Include cyber insurance requirements

STEP 5

Ongoing Monitoring Program

Vendor risk management doesn't end after onboarding. Implement continuous monitoring to detect emerging threats, track security posture changes, and ensure ongoing compliance with your security requirements.

Continuous Surveillance

Monitor vendor security news, breach reports, and threat intelligence feeds. Set up Google alerts for vendor names combined with "breach" or "security incident."

Regular Assessments

Conduct periodic security reviews based on risk tier. Reassess vendor categorization annually or after significant changes to services or data access levels.

Performance Tracking

Track key metrics including incident response times, patch management cadence, security questionnaire completion rates, and certification renewal status.

Monitoring Tools & Methods

- Third-party risk platforms (free tier options available)
- Security rating services for vendor scoring
- Annual questionnaire updates
- Quarterly business reviews for critical vendors
- Automated vulnerability scanning where possible

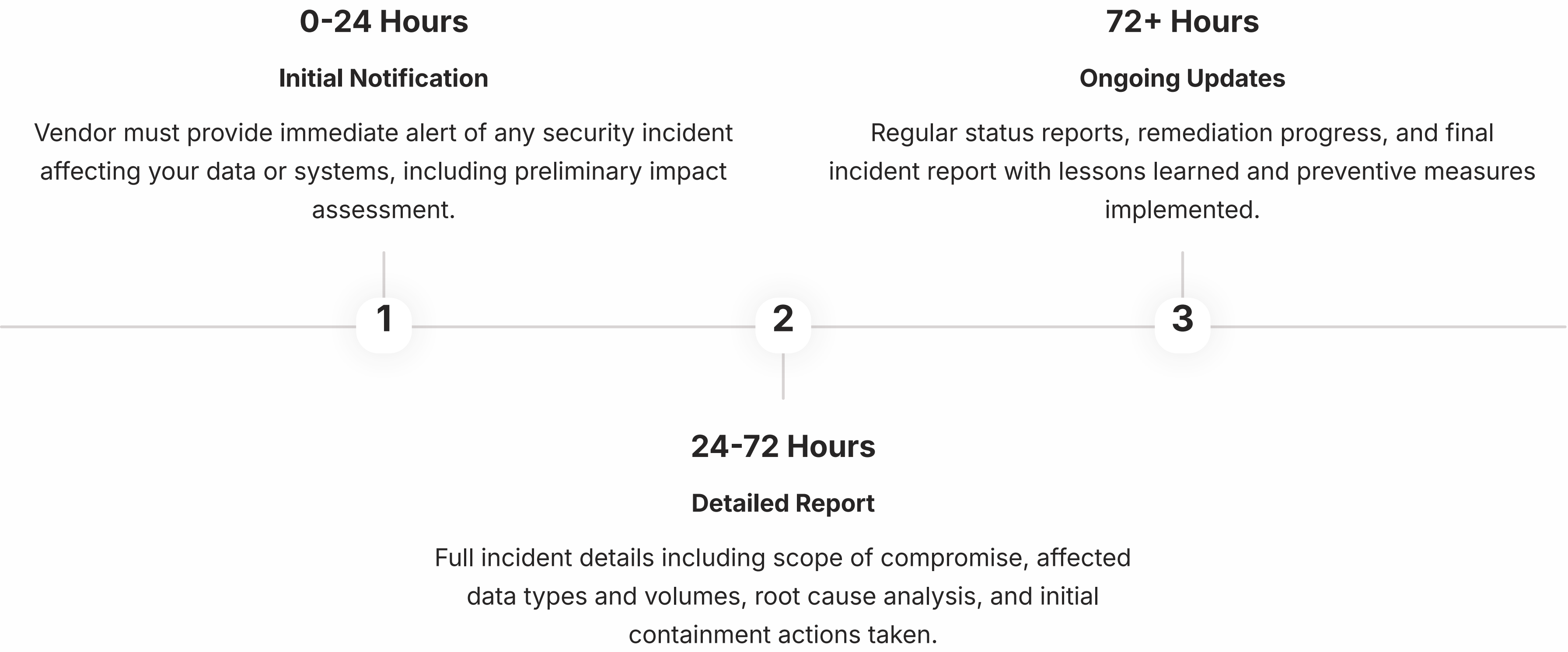
Red Flags to Watch

Unexplained service disruptions, delayed security responses, certification lapses, leadership changes in security roles, or news of financial distress requiring immediate risk reassessment.

STEP 6

Incident Notification Requirements

Clear incident notification protocols ensure you can respond quickly when vendor security events occur. Establish specific requirements that enable rapid damage assessment and containment.



1

0-24 Hours

Initial Notification

Vendor must provide immediate alert of any security incident affecting your data or systems, including preliminary impact assessment.

2

24-72 Hours

Detailed Report

Full incident details including scope of compromise, affected data types and volumes, root cause analysis, and initial containment actions taken.

3

72+ Hours

Ongoing Updates

Regular status reports, remediation progress, and final incident report with lessons learned and preventive measures implemented.

Required Incident Information

1. Nature and scope of the security incident
2. Date and time of discovery and estimated occurrence
3. Types of data potentially compromised (PII, financial, credentials)
4. Number of affected records or users from your organization
5. Immediate containment and mitigation steps taken
6. Expected timeline for full resolution and remediation
7. Vendor point of contact for ongoing incident coordination

STEP 7

Vendor Offboarding Process

Secure vendor termination is as critical as onboarding. A systematic offboarding process ensures data is returned or destroyed, access is revoked, and your security posture remains intact when relationships end.

Access Revocation

Immediately disable all vendor accounts, VPN access, and system credentials. Remove from email distribution lists and collaboration platforms. Verify deactivation in all connected systems.

Data Management

Request return or certified destruction of all company data within 30 days. Obtain written confirmation of deletion from production and backup systems. Verify compliance with data retention requirements.

Asset Recovery

Retrieve all physical assets including hardware, security tokens, access badges, and documentation. Update asset inventory and confirm return of proprietary information or intellectual property.

Documentation

Complete offboarding checklist, document lessons learned, and archive vendor security assessments. Update vendor register and notify relevant stakeholders of relationship termination.

Don't Forget

Cancel any automatic renewals, remove payment methods, update firewall rules to block vendor IP addresses, and schedule a post-offboarding security review to verify complete separation.

About Cybersecurity Non-Profit

> "Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."

Our Programs — All Completely Free

Business & Non-Profit Security

Practical guides and resources for organizations of all sizes

Family Cybersecurity

Protecting your household in the digital age

Kids Safety

Age-appropriate online safety education

Senior Digital Safety

Empowering older adults to navigate technology safely

Women's Security

Digital safety resources for women's unique challenges

Parents & Educators

Tools to teach and protect the next generation

Get Started Today

Visit **csnp.org** to access our free educational programs and join our community of security-conscious individuals and organizations.

Explore Our Resources

Download guides, templates, and tools at **csnp.org/resources** to strengthen your cybersecurity posture.