

Vendor Security Assessment Questionnaire

A comprehensive due diligence framework for evaluating third-party security practices and ensuring your organization's data remains protected throughout the vendor relationship lifecycle.



How to Use This Assessment

Questionnaire Purpose

This assessment evaluates vendor security practices across 9 critical domains. Use it during vendor onboarding and annual reviews to identify risks and ensure compliance with your security standards.

Completion Guidelines

- Provide evidence-based responses
- Include supporting documentation
- Be transparent about gaps
- Update responses as controls evolve

Scoring Framework

Each section is scored from 0-5 based on maturity and completeness. A final score determines vendor risk level and required remediation actions.

Timeline Expectations

Complete initial assessment within 10 business days.
Critical gaps must be addressed before contract execution.
Annual reassessments ensure ongoing compliance.

A background image showing a close-up of two hands shaking in a firm grip, symbolizing a business agreement or partnership. The hands are wearing white dress shirts with blue patterned sleeves. The background is a blurred office setting with a window and some greenery.

Company Information

1

Basic Details

Legal company name, primary business address, year established, number of employees, and annual revenue range.

2

Services & Data

Description of services provided, types of data accessed or stored, data classification levels, and data retention periods.

3

Contact Information

Primary contact, security officer details, legal department contact, and 24/7 incident response contact information.

Security Governance & Risk Management

Information Security Policy

Do you maintain a comprehensive, board-approved information security policy reviewed annually?

Security Leadership

Is there a dedicated Chief Information Security Officer or equivalent role with executive reporting?

Risk Assessment Program

Do you conduct formal risk assessments at least annually with documented remediation plans?

Security governance establishes the foundation for all other controls. Strong governance includes clear policies, dedicated leadership, regular risk assessments, security awareness training for all employees, and a formal third-party risk management program.

Access Control & Identity Management



Critical Access Controls

Multi-Factor Authentication: Required for all remote access and privileged accounts

Least Privilege: Users granted minimum necessary permissions

Access Reviews: Quarterly reviews of user access rights

Termination Process: Immediate access revocation upon employee departure

Password Standards: Strong password policies enforced technically

Describe your processes for provisioning, reviewing, and revoking system access across the organization.

Data Protection & Encryption

Data at Rest

All sensitive data encrypted using AES-256 or equivalent. Encryption keys managed through secure key management system with role-based access controls.

Data in Transit

TLS 1.2 or higher required for all data transmission. Certificate management program ensures valid, up-to-date certificates across all systems.

Secure Disposal

Documented data sanitization procedures following NIST 800-88 standards. Certificate of destruction provided for physical media disposal.

 Data classification program must categorize information and apply appropriate protection controls based on sensitivity level.

Network Security & Infrastructure

01

Perimeter Defense

Next-generation firewalls, intrusion detection/prevention systems, and network segmentation separating production from development environments.

03

Security Monitoring

24/7 security operations center monitoring logs, alerts, and suspicious activity with documented response procedures.

02

Vulnerability Management

Quarterly vulnerability scans, penetration testing annually, and critical patches applied within 30 days of vendor release.

04

Secure Development

Secure coding standards, code review processes, and security testing integrated throughout software development lifecycle.



Incident Response & Management

Incident Response Plan

Do you maintain a documented incident response plan tested at least annually? The plan should define roles, responsibilities, escalation procedures, and communication protocols.

Key Requirements

- Incident classification and severity levels
- 24/7 incident response team availability
- Forensic investigation capabilities
- Customer notification within 24 hours
- Post-incident review and lessons learned

Response Timeline

Detection: Automated alerts for security events

Containment: Within 2 hours of verification

Eradication: Remove threat and vulnerabilities

Recovery: Restore systems to normal operation

Communication: Timely updates to stakeholders

Business Continuity & Disaster Recovery

Business Impact Analysis

Identification of critical business functions, maximum tolerable downtime (MTD), and recovery time objectives (RTO) for each system.

Data Backup Strategy

Automated daily backups with offsite storage, encryption, and quarterly restoration testing to verify backup integrity.

1

2

3

4

Continuity Planning

Documented procedures for maintaining operations during disruptions, including alternate site arrangements and succession planning.

Testing & Validation

Annual full disaster recovery tests with documented results and improvement recommendations implemented before next test.

Compliance & Certifications



ISO 27001

International standard for information security management systems demonstrating systematic approach to managing sensitive information.



SOC 2 Type II

Independent audit of security, availability, and confidentiality controls over a minimum 6-month period.



HIPAA Compliance

For healthcare data handling: Business Associate Agreement signed, encryption standards met, breach notification procedures established.



PCI DSS

Payment Card Industry compliance if processing, storing, or transmitting cardholder data with annual validation.



GDPR Readiness

Privacy by design, data protection officer appointed, documented data processing agreements, and breach notification capabilities.



Industry Standards

Additional compliance with NIST Cybersecurity Framework, CIS Controls, or industry-specific regulatory requirements.

Provide copies of current certifications, latest audit reports, and evidence of ongoing compliance monitoring activities.



DOMAIN 6

Subcontractor Management

1

Inventory

Maintain complete list of all subcontractors with access to data or systems.

2

Assessment

Security assessments required before onboarding any subcontractor.

3

Contracts

Written agreements include security requirements and audit rights.

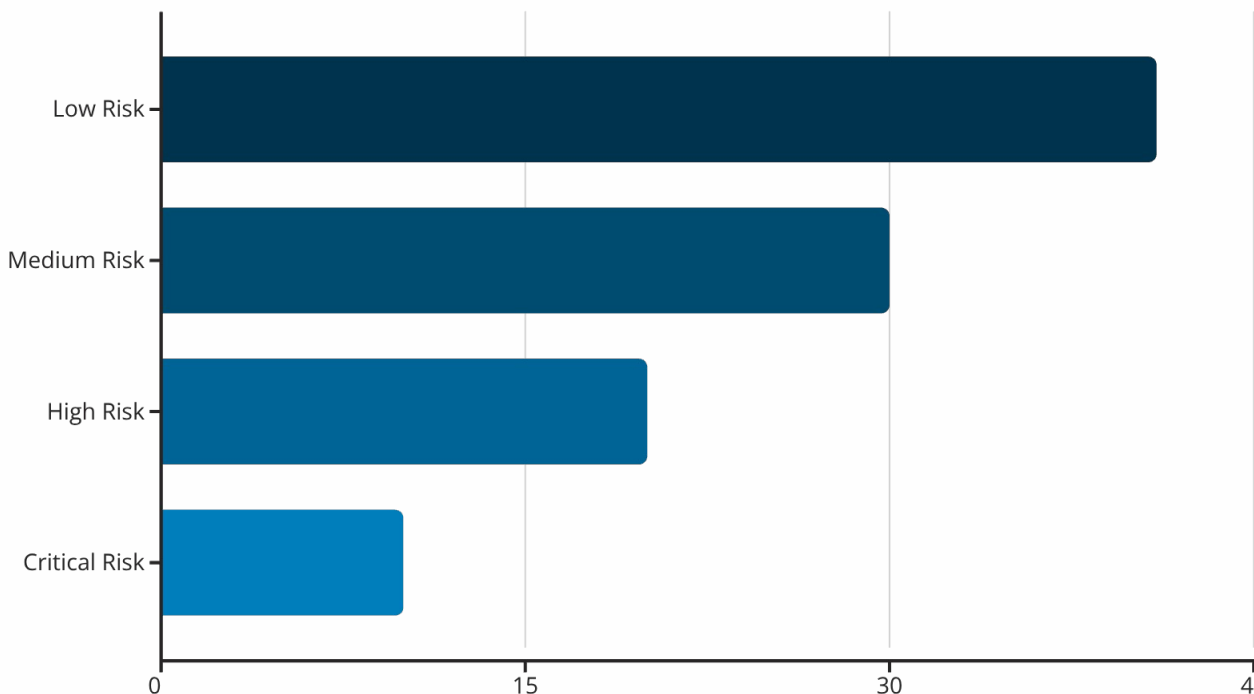
4

Monitoring

Annual reviews of subcontractor security controls and compliance.

Scoring Guide & Next Steps

Assessment Scoring



Low Risk (41-45): Approved for engagement

Medium Risk (30-40): Approved with monitoring

High Risk (20-29): Remediation plan required

Critical Risk (0-19): Engagement not recommended

About CSNP

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

Our Free Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety
- Senior Digital Safety
- Women's Security
- Parents & Educators

Website: csnp.org **Resources:** csnp.org/resources