Vendor Risk Assessment Toolkit 2026

Vendor inventory worksheet, security questionnaire, risk-tiering matrix, contractual must-haves checklist, scoring rubric, and regulatory crosswalk for SOC 2 CC9.2, HIPAA BAA, GLBA §314.4(f), CMMC RA.L2-3.11.1, and NYDFS Part 500.11.

51%
of breaches originate from a third-party vendor (IBM 2024)

WHAT IS IN THIS TOOLKIT?

QUICK START

How to Use This Toolkit

This toolkit gives you the components to run a complete vendor risk management program from scratch. Start with your top 5 critical vendors (those with access to sensitive data, core systems, or payment flows). Use the questionnaire, score them, review contracts, and schedule annual re-assessments.

1 **Populate the Vendor Inventory**
List every third-party vendor, SaaS tool, or service provider that has access to your data, systems, or networks. Include sub-processors (e.g., cloud providers your SaaS vendors use). This is your master vendor register.

2 **Tier Your Vendors (Page 4)**
Classify each vendor as Tier 1 (Critical), Tier 2 (Important), or Tier 3 (Standard) based on data sensitivity and system access. Tier 1 vendors get the full questionnaire + annual deep review. Tier 3 gets a shorter review on onboarding + biennial check.

3 **Send the Security Questionnaire (Pages 5–8)**
Send the full questionnaire to all Tier 1 vendors. Use the abbreviated version (Sections 1–4 only) for Tier 2 vendors. Tier 3 vendors complete the onboarding screen only.

4 **Score and Re-Tier (Page 9)**
Score each completed questionnaire using the rubric on Page 9. A score below 60 should trigger an escalation conversation or a remediation plan before renewing the vendor relationship.

5 **Check Contracts (Page 10)**
Verify that each Tier 1 and Tier 2 contract contains the 14 contractual must-haves. Missing items are gaps — flag them in the remediation tracker (Page 11).

6 **Schedule Annual Reviews (Page 12)**
Set calendar reminders for each vendor's annual review using the template on Page 12. Tier 1 vendors also get quarterly check-ins. No review = no renewal without escalation.

WHERE TO START

If you are starting from scratch: spend 30 minutes on the Vendor Inventory (Page 3) first. Identify your top 5 vendors by data risk. Send them the questionnaire this week.

VENDOR INVENTORY

Vendor Inventory Worksheet

List every third-party vendor with access to your systems, data, or networks. Update this register whenever a new vendor is onboarded or offboarded.

Vendor Name	Service Provided	Data Accessed	System Access	Tier (1/2/3)	Review Due

SUB-PROCESSORS

Include sub-processors — vendors that your primary vendors use. GDPR Art. 28 and many BAAs require you to identify and assess sub-processors. Ask each Tier 1 vendor for their complete sub-processor list.

WHAT TO CAPTURE FOR EACH VENDOR

- Data Accessed: Which categories of data does this vendor process? (PII, PHI, financial data, credentials, proprietary IP)
- System Access: What level of access do they have? (read-only, admin, network-level, physical access)
- Contract Status: Is there a current MSA, DPA, or BAA in place? When does it expire?
- Last Review Date: When was the last security questionnaire completed and reviewed?
- Point of Contact: Internal owner of this vendor relationship + vendor security contact

RISK TIERS

Vendor Risk-Tiering Matrix

Assign each vendor a tier based on the data they access and the business impact of a compromise. Review cadence and questionnaire depth vary by tier.

TIER 1 — CRITICAL

Criteria: Accesses sensitive PII, PHI, financial data, or payment systems. Has network-level or admin system access. Would cause significant regulatory, financial, or reputational harm if compromised.

Examples: Cloud infrastructure (AWS, Azure, GCP), HRIS / payroll processors, EHR / EMR platforms, payment processors, managed security providers (MSSPs), core banking systems.

Questionnaire: Full questionnaire (all 10 sections, Pages 5–8)

Review: Annual deep review + quarterly check-in call

Contracts: MSA + DPA/BAA required. All 14 contractual must-haves required.

TIER 2 — IMPORTANT

Criteria: Accesses non-sensitive internal data or provides business-critical SaaS tools without direct access to sensitive data. A compromise would cause operational disruption but limited regulatory exposure.

Examples: CRM platforms, project management tools, marketing automation, IT ticketing systems, communications platforms (Slack, Teams at org level), backup and DR vendors.

Questionnaire: Abbreviated questionnaire (Sections 1–4 only)

Review: Annual review + post-incident check

Contracts: MSA required. DPA if any EU/CA personal data flows.

TIER 3 — STANDARD

Criteria: No access to sensitive data or core systems. Provides commodity services. Low business impact if vendor is compromised or unavailable.

Examples: Office supply vendors, travel booking (no data integration), print vendors, one-time contractors with no system access.

Questionnaire: Onboarding screen only (6 questions)

Review: Onboarding + biennial review

Contracts: Purchase order or standard vendor agreement.

SECURITY QUESTIONNAIRE — SECTIONS 1–3

Vendor Security Questionnaire

Send this questionnaire to all Tier 1 vendors annually and to Tier 2 vendors on onboarding. Use Sections 1–4 for Tier 2. Responses map to the scoring rubric on Page 9.

Section 1: Security Program Governance

Q1. Do you have a documented Information Security Policy? (Y/N — attach or provide URL)

Q2. Do you have a designated security officer or CISO? (Name and title)

Q3. Have you completed a SOC 2 Type II audit in the past 12 months? (Attach report or summary)

Q4. Do you hold ISO 27001 certification? (Attach certificate)

Q5. Have you undergone a penetration test in the past 12 months? (Y/N — provide executive summary)

Q6. How often do you conduct security awareness training for employees? (Frequency + scope)

Q7. Do you have a formal vendor/third-party risk management program for your own vendors? (Y/N)

Section 2: Access Controls & MFA

Q1. Do you enforce multi-factor authentication (MFA) for all employees accessing production systems? (Y/N)

Q2. Do you enforce MFA for remote access and VPN? (Y/N)

Q3. Do you use phishing-resistant MFA (FIDO2/hardware key) for privileged accounts? (Y/N)

Q4. Do you follow the principle of least privilege for all system access? (Y/N — describe process)

Q5. How frequently do you conduct access reviews? (Quarterly / Semi-annual / Annual)

Q6. Do you revoke access within 24 hours of employee termination? (Y/N)

Q7. Do you maintain and review privileged access logs? (Y/N — retention period)

Section 3: Encryption & Data Handling

Q1. Do you encrypt all data at rest using AES-256 or equivalent? (Y/N)

Q2. Do you encrypt all data in transit using TLS 1.2+ ? (Y/N)

Q3. Which data residency regions apply to our data? (List countries/regions)

Q4. Do you have a documented data classification policy? (Y/N)

Q5. How long do you retain our data and in what format? (Describe retention schedule)

Q6. Do you have a documented data destruction / secure deletion procedure? (Y/N)

Q7. Are backups encrypted and stored separately from primary systems? (Y/N)

Section 4: Incident Response & Breach Notification

Q1. Do you have a documented Incident Response (IR) plan? (Y/N — describe scope)

Q2. What is your breach notification SLA to customers? (Hours — specify 24/48/72 hr)

Q3. Have you experienced a security incident or data breach in the past 24 months affecting customer data? (Y/N — if yes, describe)

Q4. Do you conduct annual tabletop exercises or IR drills? (Y/N)

Q5. Do you have cyber liability insurance? (Y/N — policy limits)

Q6. Who is our primary contact for incident notification? (Name, email, phone)

Section 5: Sub-Processor Disclosure

Q1. Do you use any sub-processors that have access to our data? (Y/N — list all)

Q2. Will you notify us before engaging a new sub-processor that will access our data? (Y/N)

Q3. Do your sub-processors meet the same security standards as you? (Y/N — describe due diligence)

Q4. Are any sub-processors located outside the US/EU? (Y/N — list countries)

Q5. Do you have DPAs or equivalent agreements with all sub-processors? (Y/N)

Section 6: Business Continuity & Disaster Recovery

Q1. Do you have a documented Business Continuity Plan (BCP)? (Y/N)

Q2. What is your Recovery Time Objective (RTO) for critical systems? (Hours)

Q3. What is your Recovery Point Objective (RPO)? (Hours — maximum data loss)

Q4. How frequently do you test your DR plan? (Annual / Semi-annual / More frequent)

Q5. Do you have geographically redundant data centers or failover capacity? (Y/N)

Q6. Have you met your published RTO/RPO in an actual incident in the past 3 years? (Y/N)

Section 7: Vulnerability Management

Q1. Do you have a vulnerability management program? (Y/N)

Q2. How frequently do you conduct vulnerability scans? (Continuous / Weekly / Monthly)

Q3. How frequently do you conduct external penetration tests? (Annual / Every 2 years)

Q4. What is your SLA for patching critical vulnerabilities (CVSS 9.0+)? (Days — target: 30 days or less)

Q5. Do you participate in a coordinated vulnerability disclosure program? (Y/N)

Q6. Do you apply security patches to all production systems within 30 days of release? (Y/N)

Section 8: Secure Software Development (SDLC)

Q1. Do you have a documented Secure SDLC policy? (Y/N)

Q2. Do you conduct static application security testing (SAST) on code before deployment? (Y/N)

Q3. Do you use software composition analysis (SCA) to detect vulnerable open-source components? (Y/N)

Q4. Do you conduct code reviews with security as a review criterion? (Y/N)

Q5. Are production and development environments strictly separated? (Y/N)

Q6. Do you perform security testing on all major releases before deployment? (Y/N)

Section 9: Physical & Environmental Security

Q1. Do your data center facilities have physical access controls? (Keycards, biometrics, guards)

Q2. Are data center access logs maintained and reviewed? (Y/N — retention period)

Q3. Do employees working remotely operate under a documented remote work security policy? (Y/N)

Q4. Are endpoint devices (laptops) encrypted and managed with MDM? (Y/N)

Q5. Do you have a documented clean desk and screen lock policy? (Y/N)

Section 10: AI / LLM Data Handling (New for 2026)

Q1. Do you use AI or large language models (LLMs) in your service delivery? (Y/N — describe use case)

Q2. Does any AI/LLM component have access to our data or process it for inference? (Y/N)

Q3. Is our data used to train or fine-tune any AI model? (Y/N — if yes, opt-out available?)

Q4. Which AI providers or models do you use? (List: OpenAI, Anthropic, Cohere, open-source, etc.)

Q5. Do you have a documented AI usage and governance policy? (Y/N)

Q6. Are AI-generated outputs reviewed by a human before acting on them in your service? (Y/N)

Q7. How do you prevent prompt injection or adversarial input attacks in AI-powered workflows? (Describe)

VENDOR ATTESTATION

Vendor Attestation Statement

I, the undersigned, certify that the responses provided in this questionnaire are accurate and complete to the best of my knowledge. I understand that any material inaccuracies may constitute a breach of our vendor agreement.

Name: _____ Title: _____

Signature: _____ Date: _____

SCORING

Questionnaire Scoring Rubric — 0 to 100 Scale

Score each section based on the vendor's responses. Total score determines the vendor's risk tier recommendation. Scores below 60 should trigger a formal remediation discussion before contract renewal.

Section	Max Points	Weight	How to Score
1. Security Governance	15	15%	SOC 2/ISO cert = 15, pen test only = 8, policy only = 4, nothing = 0
2. Access Controls & MFA	15	15%	Full phishing-resistant MFA = 15, partial = 8, password-only = 0
3. Encryption & Data Handling	12	12%	AES-256 + TLS 1.2 + DPA = 12, partial encryption = 6, none = 0
4. Incident Response	13	13%	24-hr SLA + IR plan + tabletop = 13, 72-hr SLA = 7, no plan = 0
5. Sub-Processor Disclosure	8	8%	Full list + DPAs = 8, partial = 4, unknown sub-procs = 0
6. Business Continuity	10	10%	Tested DR + RTO < 4hr = 10, documented only = 5, none = 0
7. Vulnerability Management	10	10%	Continuous scanning + 30d patch = 10, annual only = 4, none = 0
8. Secure SDLC	7	7%	SAST + SCA + code review = 7, partial = 3, none = 0
9. Physical & Environmental	5	5%	Encrypted endpoints + MDM + physical controls = 5, partial = 2
10. AI/LLM Governance	5	5%	AI policy + no training on our data = 5, partial = 2, no policy = 0
TOTAL	**100**	**100%**	

SCORE INTERPRETATION

85–100 Low Risk — Strong security posture. Recommend for Tier 1 approval with standard annual review.

70–84 Moderate Risk — Acceptable with remediation plan for gaps. Address items below 70% in each section within 90 days.

55–69 Elevated Risk — Significant gaps. Require remediation plan before renewal. Consider compensating controls or contract restrictions.

Below 55 High Risk — Unacceptable. Do not renew without substantial documented improvement. Escalate to leadership.

CONTRACT REQUIREMENTS

Contractual Must-Haves — 14 Non-Negotiable Clauses

Every Tier 1 vendor contract must include these 14 clauses. Missing clauses are compliance gaps under SOC 2 CC9.2, HIPAA §164.314, GLBA §314.4(f), and GDPR Art. 28. Flag each gap in the remediation tracker.

1. Breach Notification Window

Vendor must notify you within 24 hours (HIPAA BAA), 48 hours (NYDFS Part 500), or 72 hours (GDPR) of discovering a breach affecting your data. Specify the maximum window explicitly — do not accept "promptly" or "reasonable time."

2. Audit Rights

You have the right to audit the vendor's security controls upon reasonable notice (typically 30 days). Alternatively: vendor provides annual SOC 2 Type II or ISO 27001 audit report satisfying audit rights.

3. Right to Cure and Termination for Cause

If vendor fails to meet security standards, you have the right to require cure within 30 days and to terminate the contract for cause if not cured, without penalty.

4. Data Return and Destruction

On contract termination, vendor must return all your data in a portable format within 30 days and certify secure destruction of all copies. Specify format (CSV, JSON) and destruction standard (NIST SP 800-88).

5. Sub-Processor Approval

Vendor must receive your prior written approval before engaging any new sub-processor that will access your data. You retain the right to reject sub-processors who do not meet your standards.

6. Indemnification

Vendor indemnifies you for third-party claims arising from vendor's breach, negligence, or failure to comply with security requirements. Cap should be no less than 12 months of fees or the actual breach cost.

7. Insurance Minimums

Vendor maintains: (a) Cyber liability insurance — $1M minimum, $5M preferred for Tier 1; (b) Commercial general liability — $1M per occurrence; (c) Errors & omissions — $1M minimum.

8. Security Standards Compliance

Vendor agrees to comply with applicable security frameworks (specify: SOC 2 / NIST CSF / ISO 27001 / HIPAA / GLBA / CMMC) and to maintain the security program represented in the security questionnaire.

9. Right to Require Remediation

If an audit or incident reveals material security deficiencies, you may require vendor to remediate within a defined timeline (30–60 days for critical findings) with evidence of completion.

10. Data Processing Agreement (DPA) or BAA

GDPR Art. 28 requires a DPA for any EU personal data. HIPAA requires a BAA for PHI. GLBA and CCPA require specific contractual language for consumer financial / personal data. Attach as an exhibit.

11. Security Questionnaire Renewal

Vendor agrees to complete your security questionnaire annually (Tier 1) or biennially (Tier 2). Failure to respond within 30 days of request may be grounds for suspension of the relationship.

12. Regulatory Cooperation

Vendor cooperates with any regulatory investigation, audit, or inquiry related to your data. This includes producing records, providing witness access, and maintaining relevant data holds.

13. Incident Response Cooperation

Vendor participates in your incident response process if an incident involves their systems or your data. Defines roles, communication protocols, and evidence preservation obligations.

14. Change Notification

Vendor provides 30-day written notice of: material changes to security architecture, data handling practices, ownership changes (M&A), loss of key certifications, or significant security incidents even if our data is not directly affected.

REMEDIATION TRACKING

Vendor Remediation Tracker

Log each finding from questionnaire review, contract gap analysis, or audit. Track severity, owner, due date, and status. Present this tracker at each Tier 1 vendor quarterly check-in.

Finding	Vendor	Severity	Owner	Due Date	Status	Evidence

SEVERITY DEFINITIONS

Critical	Immediate risk of breach or regulatory violation. Remediate within 30 days or escalate to leadership for risk acceptance.
High	Significant control gap. Remediate within 60 days. Document compensating controls until resolved.
Medium	Notable gap. Remediate within 90 days as part of regular security improvement cycle.
Low	Best-practice gap. Remediate within 180 days or address in next annual review cycle.

REVIEW SCHEDULE

Annual Vendor Review Calendar Template

Set calendar reminders for each vendor. Tier 1 vendors require annual deep reviews plus quarterly check-ins. Populate this template at the start of each calendar year.

Vendor	Tier	Q1 Check-in	Q2 Check-in	Q3 Check-in	Annual Review	Contract Renewal

REVIEW CHECKLIST

What to Cover in Each Review

- [ ] Re-send security questionnaire (or review prior year responses for changes)
- [ ] Review any incidents or near-misses involving this vendor since last review
- [ ] Verify current certifications (SOC 2, ISO 27001) are within validity period
- [ ] Confirm contract is current and includes all required clauses (Page 10)
- [ ] Review sub-processor list for changes
- [ ] Assess any new AI/LLM features introduced by the vendor since last review
- [ ] Update the vendor's tier if their risk profile has changed
- [ ] Review and close any open remediation items from the tracker (Page 11)
- [ ] Confirm cyber insurance is current and limits are adequate
- [ ] Document the review: date, participants, key findings, follow-ups

REGULATORY REQUIREMENTS

Regulatory Crosswalk — Vendor Management Requirements

This crosswalk maps the questionnaire sections and contractual requirements to specific regulatory obligations. Use this when responding to auditors or preparing audit evidence.

SOC 2 Type II — CC9.2

- Vendor inventory with risk tiering (Page 3–4)
- Security questionnaire on onboarding and annually (Pages 5–8)
- Contractual protections: audit rights, breach notification, sub-processor approval (Page 10)
- Evidence: completed questionnaires, signed contracts, audit reports retained

HIPAA Security Rule — §164.314 (BAA)

- Business Associate Agreement (BAA) required for any vendor handling PHI (Page 10, Clause 10)
- BAA must include: permitted uses/disclosures, safeguard requirements, breach reporting within 24 hours
- Annual review of BAA compliance (Page 12 calendar)
- Sub-processor BAAs required: your BAA must flow down to sub-processors (Section 5 of questionnaire)

GLBA Safeguards Rule — §314.4(f)

- Select and retain service providers that maintain appropriate safeguards
- Require service providers by contract to implement appropriate safeguards
- Periodically oversee service providers by reviewing their security programs
- Evidence: vendor contracts with security requirements, annual review documentation

CMMC 2.0 — RA.L2-3.11.1 (Risk Assessment)

- Periodically assess risk to organizational operations from use of information systems
- Third-party risk assessments must cover CUI (Controlled Unclassified Information) flows
- Supply chain risk management: identify and assess sub-contractors with CUI access
- Questionnaire Sections 1–3, 5, and 7 directly support CMMC RA evidence

NYDFS Part 500 — Section 500.11

- Covered entities must evaluate and oversee security practices of third-party providers
- Written contracts must address security policies, access controls, encryption, and breach notification
- 72-hour breach notification clause required (Page 10, Clause 1)
- Annual certification requires documented third-party oversight — this toolkit is your evidence

GDPR — Article 28 (Processor Contracts)

- Data Processing Agreement (DPA) required for all processors handling EU personal data
- DPA must specify: subject matter, duration, nature of processing, purpose, data categories
- Sub-processor approval required; your DPA must flow down to sub-processors
- Right to audit: Art. 28(3)(h) requires audit rights or equivalent certification (SOC 2/ISO)

LIVE TRAINING

Put This Into Practice — Vendor Risk & Third-Party Training

The toolkit is the framework. Your team needs to understand how to evaluate vendors, spot social engineering targeting payment controls, and run tabletop scenarios that include vendor-compromise situations. That's what SecurEveryone delivers.

PERSONAL

$299

1 session · 1 hour

Individual training on vendor social engineering: how attackers impersonate vendors to compromise payments and data.

Best for: Procurement, AP, IT staff who approve ve

- Vendor impersonation attack patterns
- BEC via vendor email compromise
- Callback verification for vendor changes
- SLAM method for suspicious emails
- Certificate of completion

EXECUTIVE

$899

1 session · 90 minutes

Leadership tabletop: vendor compromise scenario, supply chain risk, and regulatory obligations for third-party oversight.

Best for: CISOs, compliance officers, procuremen

- 90-minute live facilitated session
- Vendor compromise tabletop scenario
- Supply chain risk deep-dive
- Regulatory obligations walkthrough
- Audit evidence documentation
- Dual-control vendor approval training

BUSINESS

Custom

Unlimited users · 12 months

Organization-wide vendor risk training + ongoing tabletop exercises covering all third-party attack vectors.

Best for: Companies with complex vendor ecosystems or compliance obligations

- Unlimited live sessions for 12 months
- Vendor risk + BEC combined curriculum
- Quarterly tabletop exercises
- GLBA/HIPAA/SOC 2 compliance packaging
- Policy documentation for insurers
- Annual training attestation records

BOOK A SESSION

Book vendor risk training at secureveryone.com/book. All Business-tier sessions include a post-session written summary and attendance records for auditors and insurers.

SecurEveryone LLC · 1201 North Orange Street, Wilmington, DE 19801 · +1 (302) 212-0500 · info@secureveryone.com