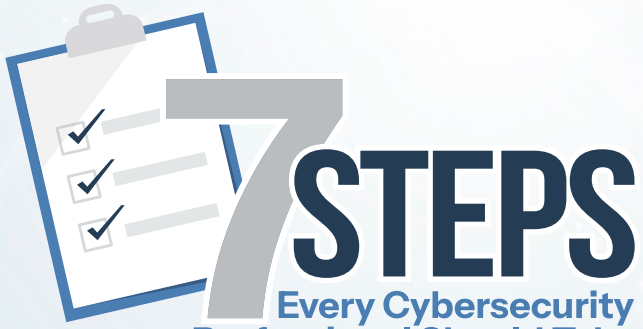
GLI® SECURE

Practitioner Guide

7 STEPS

Every Cybersecurity Professional Should Take

BEFORE ENGAGING A NEW VENDOR



7 STEPS Every Cybersecurity Professional Should Take BEFORE ENGAGING A NEW VENDOR

VENDOR SECURITY DUE DILIGENCE
PRACTITIONER GUIDE | 2026

TABLE OF CONTENTS

Introduction 1

STEP 1: Classify the Vendor by Risk Tier 2

STEP 2: Request and Review Security Certifications 3

STEP 3: Send a Risk-Tiered Security Questionnaire 4

STEP 4: Validate the Answers 6

STEP 5: Embed Security Requirements Into the Contract 7

STEP 6: Define and Enforce the Minimum Security Baseline 8

STEP 7: Add the Vendor to Your Ongoing Monitoring Program 9

Seven-Step Quick Reference Checklist 11

Why Vendor Security Programs Fail — and How to Prevent It 12

GLI Secure Vendor Security Program 13

Seven Steps Every Cybersecurity Professional Should Take Before Engaging a New Vendor

The question is not whether your vendors will be targeted by attackers. They already are. The question is whether you have done the due diligence to ensure that a vendor compromise does not become your breach — and your problem to explain to leadership, regulators, clients, and the press.

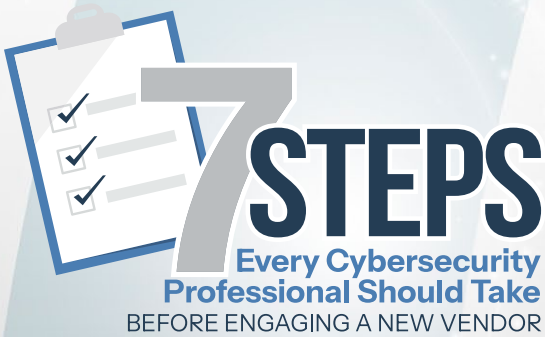
Third-party and supply chain attacks are now one of the leading causes of significant data breaches. IBM's 2024 Cost of a Data Breach Report identified third-party involvement as one of the top five factors that increase breach cost — adding an average of $512,000 to the total. The 2020 SolarWinds compromise, the 2021 Kaseya VSA attack, and countless other supply chain incidents have demonstrated that even organizations with mature internal security programs can be brought down by the security failures of a trusted vendor.

Regulatory bodies across every industry and geography have taken notice. GDPR, HIPAA, PCI DSS v4.0, DORA, NIS2, CMMC 2.0, NAIC Model Law, and dozens of other frameworks now explicitly require documented third-party risk management. The message from regulators is consistent: you are responsible for the security posture of every vendor you connect to your environment.

The following seven steps represent a practical, scalable due diligence framework that cybersecurity professionals can apply to any new vendor engagement — regardless of industry, organization size, or regulatory context. They are sequenced deliberately: each step builds on the one before it, and skipping steps undermines the value of the steps that follow.

PLEASE NOTE

These seven steps apply to all vendor categories: technology providers, software-as-a-service platforms, managed service providers, cloud infrastructure vendors, professional services firms with system access, payment processors, data analytics providers, HR technology platforms, and any other third party with access to your systems, networks, or data.



1 Classify the Vendor by Risk Tier Before You Ask a Single Question.

Effective vendor security due diligence starts with proportionality. Applying a comprehensive 60-question security assessment to a low-risk SaaS tool wastes limited security team resources and creates friction that undermines program adoption. Applying a cursory review to a vendor with privileged access to your production systems is a material risk management failure.

Before any assessment activity begins, classify the prospective vendor into a risk tier based on the nature of their access and data exposure. This single step determines the depth of due diligence required and ensures your security team's time is allocated where the risk is highest.

TIER	CRITERIA	DUE DILIGENCE LEVEL
CRITICAL (Tier 1)	Direct network or system access to production environments; processes or stores sensitive personal data at scale; provides security-critical services; involved in payment processing; part of your core operational infrastructure	Full assessment: security questionnaire, evidence review, certification verification, penetration testing evidence, on-site or virtual architecture review for highest-risk vendors. Annual reassessment
HIGH (Tier 2)	Processes limited sensitive data; indirect access to internal systems; provides services that could affect data integrity or availability	Security questionnaire, evidence review, current certification required (SOC 2 Type II or ISO 27001). Semiannual reassessment
MEDIUM (Tier 3)	No sensitive data access; access limited to non-critical internal systems; lower business impact if compromised	Abbreviated security questionnaire. Annual reassessment
LOW (Tier 4)	No system access; no data processing; purely commercial or administrative relationship	Standard commercial due diligence only. No formal security assessment required

Document your tier classification decision and the criteria that drove it. If your organization is subject to regulatory oversight — under HIPAA, PCI DSS, DORA, NIS2, CMMC 2.0, or similar frameworks — your vendor risk classification methodology itself may be subject to audit. A defensible, documented rationale for every classification decision is essential.

PRACTICAL TIP

Build your risk tier criteria into a simple intake form that any business unit can complete when requesting a new vendor. This shifts the initial classification work away from the security team and creates a consistent, auditable record of every vendor evaluation request.

7 STEPS Every Cybersecurity Professional Should Take BEFORE ENGAGING A NEW VENDOR

2 Request and Review Current Security Certifications

Before investing time in a detailed questionnaire, request whatever current security certifications the vendor holds. Certifications do not replace a security assessment — a vendor can hold an ISO 27001 certificate with a scope that excludes the systems you care about — but they establish a baseline, signal the maturity of the vendor's security program, and allow you to reduce the scope of detailed questioning where relevant, current certifications already provide assurance.

Key Certifications to Request

SOC 2 Type II Report

- Must be current — issued within the past 12 months for the period to be meaningful
- Request the full report, not a summary certificate — the auditor's description of the system, the trust service criteria tested, and any exceptions noted are critical reading
- Verify that the trust service criteria and scope cover the systems and services relevant to your engagement

ISO/IEC 27001 Certificate

- Verify currency and confirm the certificate was issued by an accredited certification body (check the accreditation body's public registry)
- Review the scope statement carefully — ISO 27001 scope can be intentionally narrow

PCI DSS Attestation of Compliance (AoC) or Report on Compliance (RoC)

- Required for any vendor involved in payment card data processing, transmission, or storage
- Confirm the service provider level and that your specific use case falls within the assessed scope

Independent Penetration Testing Reports

- Most recent report, conducted within the past 12 months, by a qualified independent third party
- Request the executive summary and, for Tier 1 vendors, evidence of remediation for any critical or high-severity findings

Additional Certifications Relevant by Industry or Geography

- HITRUST CSF (healthcare) — a composite framework that encompasses HIPAA, ISO 27001, and other standards
- FedRAMP Authorization (US government and government contractor supply chains)
- CSA STAR Certification (cloud service providers)
- Cyber Essentials / Cyber Essentials Plus (UK public sector supply chain)

PLEASE NOTE

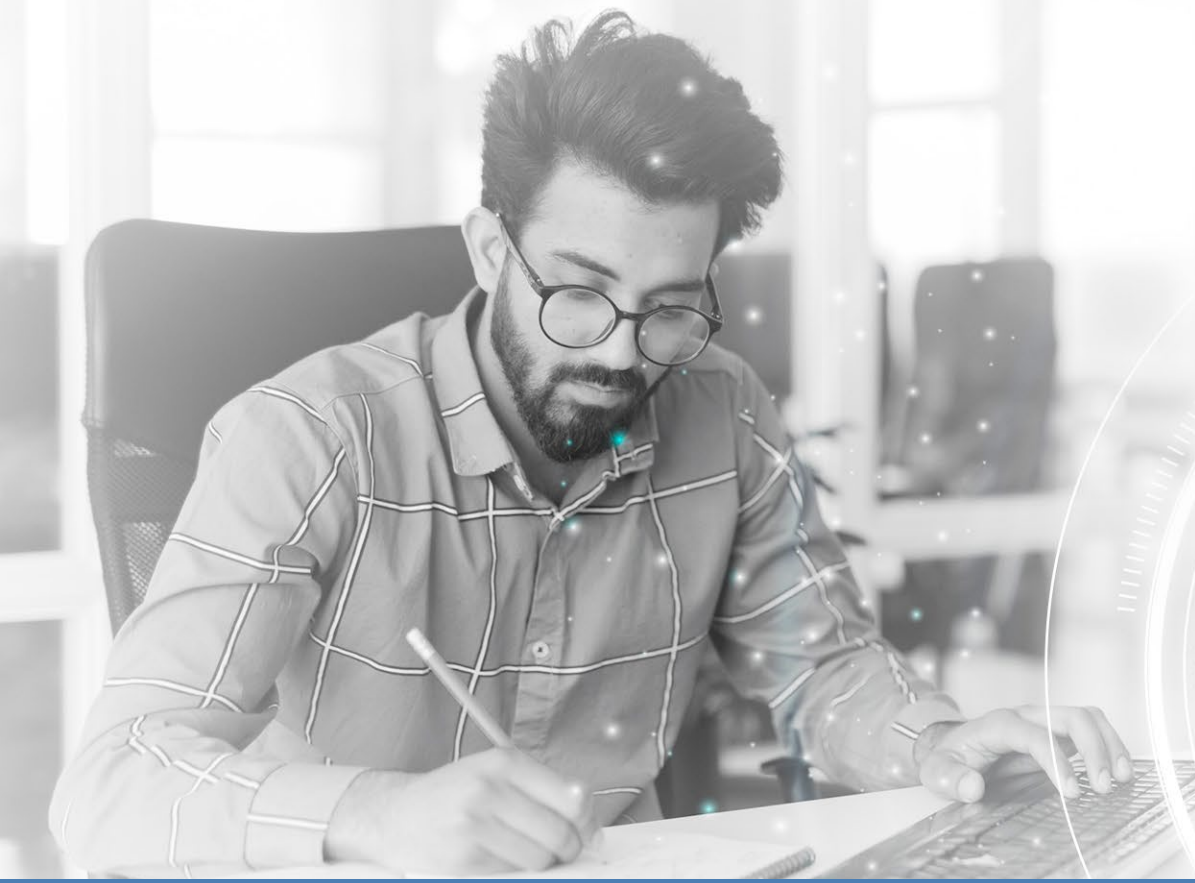
A Tier 1 or Tier 2 vendor who cannot provide a current SOC 2 Type II report or equivalent certification should be treated as a material risk finding. This does not necessarily mean declining the vendor — but it means the absence of certification must be documented, escalated, and compensated for through enhanced contractual protections and more frequent reassessment.

7 STEPS
Every Cybersecurity Professional Should Take
BEFORE ENGAGING A NEW VENDOR

3 Send a Risk-Tiered Security Questionnaire

A security questionnaire is the primary instrument for gathering structured information about a vendor's security program. The questionnaire should be proportionate to the vendor's risk tier — a 15-question abbreviated form for Tier 3 vendors, a comprehensive domain-by-domain assessment for Tier 1 vendors — and should be tailored to the specific nature of the vendor's access to your environment.

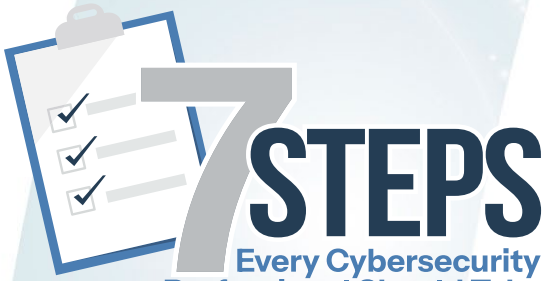
Establish a consistent scoring methodology for questionnaire responses — typically a 1-5 maturity scale per control domain — so that results can be compared across vendors, tracked over time, and presented to auditors as evidence of a systematic assessment program. Most organizations use one of the established industry questionnaire standards (SIG, CAIQ, or a custom internal standard) as the basis for their vendor questionnaire.



PRACTICAL TIP

Standardize on a single questionnaire format across your organization and maintain a library of vendor responses. When the same vendor is evaluated by multiple business units, or when a vendor is reassessed in subsequent years, the ability to compare responses side-by-side reveals changes in security posture that individual assessments miss.

DOMAIN	KEY QUESTIONS TO ASK
SECURITY PROGRAM GOVERNANCE	Do you have a documented information security policy approved by executive leadership? Who is accountable for information security at the executive or board level? When was your last independent security risk assessment, and what framework was used?
ACCESS CONTROL & IDENTITY	How do you manage privileged access to systems that interact with our environment or data? What multi-factor authentication (MFA) is enforced for remote access? How are user accounts deprovisioned when employees leave? Do you use a Privileged Access Management (PAM) solution?
ENCRYPTION & DATA PROTECTION	How is sensitive data encrypted in transit and at rest? What encryption standards are applied? How are encryption keys managed and rotated? Do you use our data for any purpose beyond the contracted service?
VULNERABILITY MANAGEMENT	How frequently do you conduct vulnerability scanning of systems within scope of our engagement? What is your process for remediating critical and high-severity vulnerabilities? What is your target remediation SLA by severity?
INCIDENT DETECTION & RESPONSE	Do you have a documented incident response plan? What is your contractual notification timeline for security incidents affecting our environment or data? Who is your designated security contact for incident communication?
SUBPROCESSORS & FOURTH PARTIES	Do you use any subprocessors or sub-contractors with access to our data or systems? Who are they? Have they been security assessed using your vendor risk program? What are your contractual flow-down security obligations to them?
PHYSICAL & ENVIRONMENTAL SECURITY	How do you control physical access to facilities where our data is processed or stored? Are data centers independently audited? What environmental controls protect against power, cooling, and physical threats?
BUSINESS CONTINUITY & RESILIENCE	What are your documented Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for services relevant to our engagement? Have you tested your disaster recovery plan in the past 12 months, and what were the results?
DATA HANDLING & RETENTION	Where is our data physically stored (country/region)? What are your data retention periods and deletion processes? How do you handle data subject access requests that involve our data? What happens to our data upon contract termination?
REGULATORY & COMPLIANCE	What security or data protection frameworks are you currently certified or compliant against? Are you subject to any specific data protection regulations (GDPR, HIPAA, CCPA, etc.) relevant to our engagement? Have you had any regulatory enforcement actions or material audit findings in the past three years?



7 STEPS
Every Cybersecurity Professional Should Take
BEFORE ENGAGING A NEW VENDOR

4 Validate the Answers — Do Not Accept Questionnaire Responses at Face Value

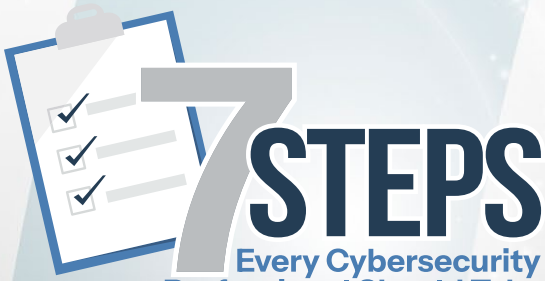
Security questionnaire responses are self-reported. They reflect what a vendor's sales or compliance team believes reviewers want to see, not necessarily the operational reality of their security program. For Tier 1 and Tier 2 vendors, validation of questionnaire responses is not optional — it is the step that separates genuine due diligence from a documentation exercise.

Validation Methods by Vendor Tier

- **Evidence requests** — for critical controls, request supporting documentation: security policies, recent penetration test executive summaries, system architecture diagrams, access control process documentation, sample audit logs.
- **Certification verification** — do not rely on vendor-provided certificate images; cross-reference ISO 27001 certificates against the issuing accreditation body's public registry; verify SOC 2 reports were issued by a PCAOB-registered or equivalent auditing firm.
- **Technical spot-checks** — for vendors with internet-facing systems, conduct passive reconnaissance to identify obvious security gaps (exposed services, certificate issues, known vulnerability disclosures) that contradict questionnaire responses.
- **Independent security assessment** — for Tier 1 vendors, consider commissioning a GLI Secure vendor security assessment, which includes an architecture review and limited penetration test of the integration boundary between your environment and the vendor's.
- **Public breach and vulnerability research** — search breach disclosure databases, CVE records, and security news archives for the vendor's name; a vendor with undisclosed incidents in their questionnaire responses is a significant finding.
- **Reference checks** — speak directly with another client of the vendor, ideally in a similar industry or regulatory context, about their experience with the vendor's security responsiveness and incident communication.

PLEASE NOTE

Research consistently shows that a significant percentage of questionnaire responses contain inaccuracies — some deliberate, many simply reflecting a gap between documented policy and operational practice. The validation step is where the real picture emerges. For any critical finding that emerges during validation, document it, communicate it to the vendor, and determine whether it is a deal-breaker or a remediation needed before contract execution.



5 Embed Security Requirements Into the Contract Before Signature

The contract is your primary enforcement mechanism for vendor security behavior. Once it is signed without cybersecurity provisions, your ability to mandate security standards, require breach notification, audit security controls, or enforce data handling obligations is severely constrained. Security clauses are not optional add-ons to be negotiated away for commercial reasons — they are essential risk management terms that protect your organization and, in many regulatory frameworks, are legally required.

Minimum Contractual Security Requirements

- **Incident notification obligation** — specify the exact timeframe within which the vendor must notify you of any security incident that affects, or may affect, your environment, systems, or data. Align this window to your own regulatory notification obligations — many frameworks require you to notify a regulator or affected individuals within 24 to 72 hours of becoming aware of a breach, and you cannot do so if your vendor takes days to tell you.
- **Right to audit** — reserve the right to conduct or commission an independent security assessment of the vendor at your discretion, on reasonable notice, at no additional cost. This clause is frequently resisted by vendors; its presence in the contract signals the seriousness of your security requirements and creates a credible deterrent against security degradation.
- **Data processing and protection obligations** — define precisely what data the vendor may access, process, and store; the security standards applicable to that data; retention limitations; and deletion obligations upon contract termination or on your request.
- **Subprocessor and fourth-party restrictions** — require the vendor to obtain your prior written consent before engaging any subprocessor with access to your data or systems. Require flow-down of your security requirements to all approved subprocessors.
- **Security standards maintenance** — require the vendor to maintain their stated security certifications (SOC 2 Type II, ISO 27001, PCI DSS, or other applicable standards) throughout the contract term and to notify you within a defined period if any certification lapses, is suspended, or is materially modified.
- **Independent penetration testing** — require the vendor to conduct annual independent penetration testing of systems within scope of your integration and to provide a summary of results and remediation evidence upon request.
- **Regulatory cooperation** — require the vendor to cooperate fully with any regulatory audit, inspection, or investigation that involves their services or systems, including providing documentation and making personnel available for interviews.
- **Cyber liability insurance** — require the vendor to maintain cyber liability insurance at a minimum coverage level appropriate to the risk they represent, and to name you as an additional insured where applicable.
- **Termination rights for security cause** — include provisions that allow you to terminate the contract for material security failures, breach of security obligations, or loss of required certifications, without penalty.

PRACTICAL TIP

Engage legal counsel to review your cybersecurity contract clauses — and push back firmly when vendors attempt to strike security provisions during negotiations. A vendor who resists reasonable security contract terms is telling you something important about how seriously they take security obligations.

7 STEPS
Every Cybersecurity Professional Should Take
BEFORE ENGAGING A NEW VENDOR

6 Define and Enforce the Minimum Security Baseline for Access Provisioning

The contract is signed. The security assessment is complete. Yet this is where many vendor security programs fail. Access is provisioned without applying the security requirements identified during assessment. Before any vendor is given access to your systems, networks, or data, a minimum security baseline should be defined, communicated, verified, and recorded in the vendor register. This record should include the systems and permissions granted, the MFA method, whether privileged access management (PAM) is used, and the next access review date. It provides essential evidence for audits and incident response.

Minimum Access Security Baseline

- **Principle of least privilege** — vendor access must be scoped to the minimum systems, data, applications, and permissions required to deliver the contracted service. Every permission beyond that minimum is unnecessary risk. Review and challenge every access request against this principle before approving it.
- **Multi-factor authentication (MFA**) — all vendor remote access must require MFA. For Tier 1 and Tier 2 vendors with access to sensitive systems or data, phishing-resistant MFA (FIDO2, hardware security keys, or certificate-based authentication) should be required. SMS-based one-time codes are not sufficient for high-risk vendor access.
- **Privileged Access Management (PAM)** — vendor privileged access to critical systems should be mediated through a PAM solution that enforces session recording, just-in-time access provisioning, and automatic session termination. This provides both a deterrent against misuse and an audit trail for incident investigation.
- **Time-limited and task-scoped access windows** — where possible, provision vendor access for specific, defined maintenance or delivery windows rather than as permanent standing access. Access that is not actively being used should not exist.
- **Network segmentation** — vendor connections should terminate in a dedicated network zone isolated from your core production environment. Direct vendor access into your primary internal network is a significant risk that network architecture should prevent, not just policy.
- **Access logging and monitoring** — all vendor access activity must be logged to a centralized logging system (SIEM or equivalent) with alerting configured for anomalous access patterns: access outside normal business hours, access to systems outside the defined scope, privilege escalation attempts, and bulk data access or export.
- **Unique credentials per vendor** — never share credentials between vendors or between vendor and internal users. Each vendor relationship must have its own unique, auditable credential set.
- **Access review cadence** — vendor access privileges must be formally reviewed at a defined interval (quarterly for Tier 1, semiannually for Tier 2). Any access privilege unused within 90 days should be automatically revoked pending justification.

PLEASE NOTE

The most sophisticated vendor access controls in the world are undermined by a single IT help desk interaction that provisions access without verifying identity. Your access provisioning procedures — and the security awareness of every person who can create or modify vendor credentials — are as important as the technical controls themselves.

7 STEPS
Every Cybersecurity Professional Should Take
BEFORE ENGAGING A NEW VENDOR

7 Add the Vendor to Your Ongoing Monitoring Program

Vendor due diligence is not a one-time checkpoint that ends when access is provisioned. A vendor that was secure and compliant at the time of onboarding may experience a significant security incident six months later, may allow a security certification to lapse, may be acquired by a company with materially different security standards, or may expand their services in ways that create new risk to your environment.

Ongoing Monitoring Activities

- **Periodic reassessment** — schedule formal security reassessments for all vendors at intervals appropriate to their risk tier. Tier 1 vendors should be fully reassessed annually. Tier 2 vendors annually with abbreviated scope. Tier 3 vendors every two years. Any vendor involved in a security incident — their own or one affecting their industry — should trigger an unscheduled out-of-cycle reassessment regardless of tier.

- **Certification expiry tracking** — maintain a calendar or automated alert system for the expiry dates of all vendor security certifications. A SOC 2 Type II report that covers a period ending 18 months ago is no longer meaningful assurance. Alert your team 90 days before any critical vendor certification expires and require renewal documentation before the expiry date.

- **Threat intelligence and breach monitoring** — use threat intelligence feeds, dark web monitoring services, or security news tracking to receive alerts when vendors appear in breach disclosures, credential dumps, ransomware victim lists, or vulnerability disclosures. Set up Google Alerts or equivalent notifications for your most critical vendors. A vendor breach that you learn about from the news rather than from the vendor is a contractual notification failure as well as an operational risk.

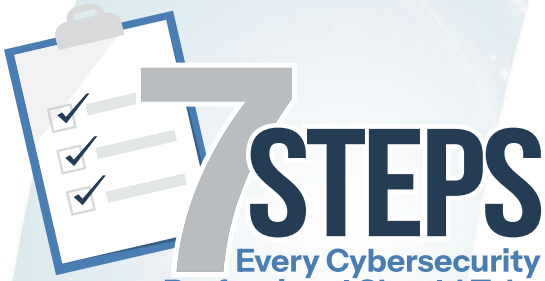
- **Material change notifications** — your vendor contract should require vendors to notify you of material changes to their security posture: changes to subprocessors, significant changes to their security architecture or controls, ownership changes, or any regulatory enforcement action against them. Track these notifications as part of your vendor risk register.

- **Regulatory and industry news monitoring** — regulatory guidance, enforcement actions, and industry-specific cybersecurity developments can materially change the risk profile of specific vendor categories. A new regulation that applies to a class of vendors you use, or a regulatory action against a vendor in your sector, should trigger a review of your own vendor relationships in that category.

- **Access recertification** — independently of your broader vendor reassessment cycle, formally recertify all vendor access permissions on a quarterly basis for Tier 1 vendors and semiannually for Tier 2. This review should confirm that access is still required, still scoped appropriately, and that the vendor's security posture has not materially degraded since the last review.

PLEASE NOTE

Integrate vendor monitoring into your SIEM alerting, security calendar, and program reporting — not into a spreadsheet that someone reviews when they have time. Manual monitoring processes are the first thing to fail when teams are busy, and teams are always busiest precisely when a vendor incident requires the fastest response.



The final step in the vendor engagement process is the beginning of an ongoing relationship with vendor security as a continuous program function — not a periodic project.

MONITORING ACTIVITY	TIER 1 (Critical)	TIER 2 (High)	TIER 3 (Medium)
FULL SECURITY REASSESSMENT	Annual	Annual	Every 2 years
CERTIFICATION STATUS CHECK	Quarterly	Semiannually	Annually
BREACH & THREAT INTELLIGENCE MONITORING	Continuous	Monthly review	Quarterly review
ACCESS PRIVILEGE RECERTIFICATION	Quarterly	Semiannually	Annually
CONTRACT TERMS REVIEW	Annually	Annually	At renewal
OUT-OF-CYCLE TRIGGERED REVIEW	Any security incident, material change or regulatory action	Any security incident	Any security incident

Seven-Step Quick Reference Checklist

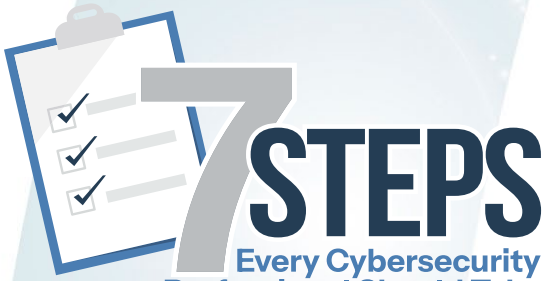
Use this checklist as a pre-approval gate before any new vendor receives access to your systems, networks, or data:

NO.	STEP	ACTION REQUIRED BEFORE VENDOR ACCESS IS APPROVED
1	☐ Classify	Assign vendor to risk tier (Critical / High / Medium / Low) based on access and data criteria. Document the classification rationale.
2	☐ Certify	Request and verify current security certifications (SOC 2 Type II, ISO 27001, PCI DSS AoC, and any industry-specific certifications). Confirm currency and scope.
3	☐ Assess	Send risk-tiered security questionnaire. Receive completed, signed responses. Score against your standard criteria.
4	☐ Validate	Request supporting evidence for critical controls. Conduct independent verification for Tier 1 and Tier 2 vendors. Document and escalate any material findings.
5	☐ Contract	Confirm cybersecurity contract clauses are included and agreed before contract execution: incident notification, right to audit, data processing obligations, subprocessor restrictions, certification maintenance, penetration testing requirements, termination for security cause.
6	☐ Provision	Define and document minimum access security baseline before provisioning: least privilege scope, MFA enforcement, PAM for privileged access, network segmentation, access logging, access review schedule.
7	☐ Monitor	Add vendor to ongoing monitoring program: set reassessment date, certification expiry calendar alerts, breach monitoring, access recertification schedule.

Why Vendor Security Programs Fail — and How to Prevent It

Even organizations that adopt all seven steps encounter common implementation failures that undermine the program's effectiveness. Awareness of these failure modes is the first step to preventing them.

COMMON FAILURE MODE	PREVENTION
Assessments completed but findings never tracked to remediation	Build a findings tracker integrated into your vendor risk register. Every material finding requires a documented remediation commitment, owner, and target date.
Program applies only to net-new vendors, not existing ones	Backfill your existing vendor population through a tiered remediation approach: assess all Tier 1 vendors first, then Tier 2, within a defined program timeline.
IT provisions access without security team involvement	Establish a formal vendor access request workflow that routes through the security team before credentials are provisioned. No access without security sign-off.
Questionnaire responses accepted without evidence review	Establish a policy: Tier 1 vendors require evidence for all critical controls. Tier 2 requires evidence for controls with 'not implemented' or 'partially implemented' responses.
Monitoring schedule exists on paper but not in practice	Integrate monitoring activities into your security calendar, SIEM alerting, and ticketing system. Calendar entries and automated alerts are more reliable than human memory.
Security clauses absent or struck from vendor contracts	Brief your legal and procurement teams on the non-negotiable cybersecurity clauses. Document any deviations as risk acceptances requiring CISO or executive sign-off.
Program is treated as a security team function, not a business function	Vendor security program governance should include stakeholders from legal, procurement, IT, and the relevant business unit — not just the security team.



GLI Secure Vendor Security Program Services Include:

- **Vendor Security Program design:** policy, procedures, risk tier criteria, questionnaire library, scoring methodology, and governance framework
- **Vendor assessment execution:** questionnaire distribution, evidence review, validation testing, and findings reporting for your vendor population
- **Contract clause library:** standard cybersecurity contract language reviewed by legal counsel and updated for current regulatory requirements
- **Ongoing monitoring management:** certification tracking, breach intelligence monitoring, and access recertification support
- **Regulatory evidence packaging:** vendor program documentation formatted for audit presentation under HIPAA, PCI DSS, DORA, NIS2, CMMC 2.0, SOC 2, and other applicable frameworks
- **vCISO integration:** vendor program management delivered as part of a GLI Secure Virtual CISO engagement for organizations that need full security program leadership

GLI Secure Can Build and Run Your Vendor Security Program

If the seven steps above describe work your security team does not currently have the capacity, tools, or expertise to execute consistently, GLI Secure can help. Our Vendor Security Program services cover the full vendor engagement lifecycle — from initial risk tiering and assessment through ongoing monitoring and regulatory evidence packaging — for organizations across every industry and geography.

Ask us about the GLI Secure Vendor Security Program Assessment:

INQUIRE HERE

Learn about our fixed-fee, 15-business-day engagement that delivers a complete inventory of your current vendor estate, a risk-tiered vendor register, a gap analysis against your applicable regulatory third-party requirements, and a recommended program design. No surprises, no ongoing commitment required.

GLI® GAMING LABORATORIES INTERNATIONAL®

ILLUMINATING YOUR PATH **TO GREATNESS**

gaminglabs.com/cybersecurity | getstarted@gaminglabs.com