VENDOR RISK ASSESSMENTS: A STEP-BY-STEP GUIDE

The close associations with vendors, contractors, and partners introduce substantial cybersecurity, privacy and compliance risks if vendor environments lack appropriate safeguards. Recent research indicates 60% of businesses suffered a breach stemming from a third-party vendor deficiency over the past two years. Weak vendor security profoundly threatens the confidentiality, integrity and availability of your own data and systems when integrating solutions into your environment.

Managing this growing vendor-driven risk surface requires implementing a robust vendor risk assessment program to thoroughly evaluate third parties before onboarding and consistently thereafter. Structured assessments examine vendor security practices, controls, and protections around data handling to identify gaps that could expose your organization.

By establishing standards through risk-based questionnaires, document reviews, audits, and testing, you gain visibility into deficiencies requiring remediation by vendors before integration proceeds. Conducting rigorous pre-contracting evaluations reduces the likelihood of partnering with vendors who lack cybersecurity fundamentals.

This article provides a step-by-step guide to instituting a vendor risk assessment program, the key phases involved, criteria for evaluation, and best practices for ongoing monitoring and reviews. With a methodical process powered by automation and human review, you can effectively assess and manage third-party cyber risk to avoid devastating financial, reputational and legal consequences.

DEFINE ASSESSMENT SCOPE AND CRITERIA

The first step is determining the scope of vendors to assess and establishing focused risk criteria tailored to your security priorities.

Define Vendor Inclusion Criteria

The assessment process should initially focus on vendors handling sensitive data or interconnecting with your network. This includes:

- Cloud service providers with access to confidential data
- Utilities and infrastructure supporting operations
- IT and security vendors with administrative access
- Partners integrating solutions into your environment
- Contractors accessing internal systems
- Any third party storing or processing protected data

Formalize objective criteria and thresholds for inclusion based on data access and system permissions granted.

Establish Risk Categories and Parameters
Create standards by mapping vendor practices to defined risk categories aligned with your cyber priorities and industry frameworks like the NIST CSF. Sample risk areas include:

- *Data Security:* Encryption, access controls, classification, retention and disposal
- *Application Security:* Development practices, testing, change control, vulnerability management
- *Network Security:* Perimeter controls, segmentation, monitoring, protocols
- *Endpoint Security:* Device hardening, patching, malware prevention
- *Identity Management:* Authentication, authorization, access administration
- *Physical Security:* Visitor management, surveillance, data center protections
- *Business Continuity:* Backup systems, redundancy, disaster recovery
- *Compliance Controls:* Data privacy, regulations, legal commitments

Tailor by Data Sensitivity
Tier assessment stringency for vendors according to the sensitivity of data exchanged. Use your data classification scheme to dictate proportional requirements.

Align to Internal Security Standards
Ensure assessment criteria map directly to your internal policies, frameworks and controls to obligate vendors to matching rigor.

Vendor Risk Criteria
Properly scoped criteria customized to your environment enables risk-based evaluations.

COLLECT INFORMATION FROM VENDORS

Next, gathering comprehensive evidence from vendors on their security posture is required to perform assessments. Key techniques include:

Utilize Standardized Disclosures or Questionnaires
Develop extensive disclosures spanning control areas in your criteria. Require details on:

- Organizational security programs and frameworks followed
- Technical controls and safeguards in place
- Asset and data management protocols
- Auditing practices
- Access and identity administration
- Incident response capabilities
- Compliance adherence
- Subcontractor management

Promote completeness by requiring explanations of how vendors meet specific standards outlined in your criteria.

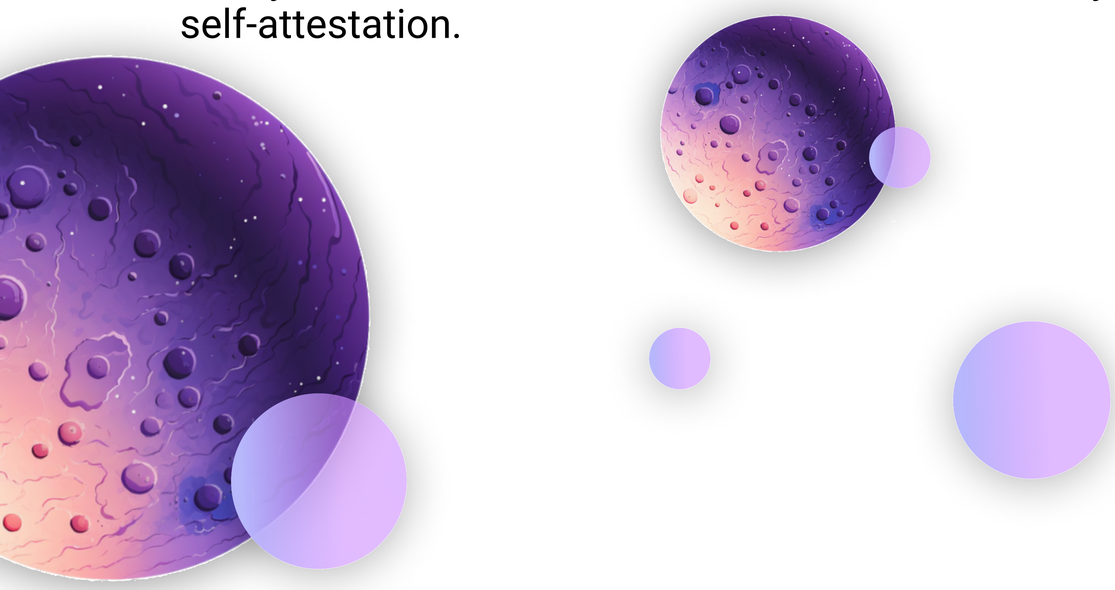
Request Documentation for Review
Demand supporting documentation like audits, policies, procedures, system configurations, architecture diagrams, and security process documentation. Assessing artifacts validates that program elements are formally defined and operational versus just claims.

Conduct Interviews
Schedule calls with vendor security staff to probe their expertise across your control domains. Assess their overall cyber maturity through informed dialogue.

Perform On-site Assessments
For vendors handling highly sensitive data, on premises assessments led by your IT audit team provide assurance regarding their enacted controls and processes.

Require Independent Audits
Mandate regular comprehensive cybersecurity audits conducted by accredited third party firms to identify control gaps. Review the results.

Evaluate Against Standards
Assess vendor security against applicable frameworks like ISO 27001, NIST CSF, or industry-specific standards. By collecting exhaustive evidence and assessing vendors against rigorous criteria, you gain clarity on their actual effectiveness versus a cursory self-attestation.



ANALYZE AND SCORE RISK LEVELS

With information gathering complete, structured analysis against defined criteria determines inherent risk levels, identifies gaps, and guides remediation.

Objectively Evaluate Against Criteria
Have your IT auditors systematically assess vendor documentation, responses, and evidence against your program criteria. Identify areas fully meeting standards versus deficiencies.

Categorize Inherent Risk
Classify vendor inherent cyber risk given their current control deficiencies into high, moderate, low tiers that dictate your response requirements.

Determine Residual Risk
Estimate their residual risk after planned controls and continuing oversight are applied. This reveals the true ongoing exposure from partnering.

Quantify Compliance Gaps
Note whether vendor controls fully meet legal and regulatory compliance obligations associated with your industry and data types.

Calculate Overall Cyber Risk Score
Derive an overall risk score based on assessments across control domains.

Prioritize Remediations
Identify and prioritize gaps requiring remediation by vendors by:

- Risk severity (High/Critical Gaps)
- Compliance failures
- Controls on sensitive data flows

Verification against rigorous criteria separates strong controls from unsatisfactory vendor risk requiring attention.

DOCUMENT AND COMMUNICATE FINDINGS

Conveying assessment results to vendors and internal leadership is critical for addressing identified shortcomings.

Produce Risk Assessment Report
Generate a detailed report specifying:

- Review methods and scope
- Criteria assessments across control domains
- Notable gaps and vulnerabilities identified
- Prioritized remediation recommendations
- Final risk scores and tiered ratings

ETHICO

Contact Us for More Information | 800-859-8840 sales@ethico.com
www.ethico.com

Present Findings to Vendor
Share report with the vendor to validate accuracy and jointly discuss improvement opportunities. Be prescriptive in required enhancements like implementing technologies, processes, testing, audits or training.

Enforce Remediation
In contract negotiations, make mitigating major deficiencies a mandatory condition of partnership with timeline expectations.

Maintain Assessment Records
Documenting assessments each year provides visibility into vendor risk trajectories to identify backsliding.

Brief Leadership on Risks
Keep executive sponsors apprised of residual risk levels for vendor partnerships that could impact operations. Escalate critical gaps requiring vendor commitments or added safeguards.

Enable Risk-Based Decisions
Equip procurement and vendor managers with risk insights to determine partnership suitability and guide terms. Provide board oversight on overall vendor risk exposure. Assessments inform risk mitigation and ensure responsibilities for acting are clear internally and externally.

MONITOR AND REVIEW REGULARLY

The vendor assessment process does not end once initial due diligence is complete. Regular reviews and monitoring provides ongoing assurance as partnerships evolve.

Enforce Remediation Commitments
Gain vendor sign-off on mandated enhancements with timeframes for implementation. Follow-up frequently to validate completion and request evidence.

Require Security Audits
Incorporate annual audits by accredited firms into contracts to identify new issues arising. Review results using your criteria.

Schedule Regular Assessments
Conduct full assessments annually to address changes in scale, environment, data access and technologies. Quarterly checkpoint calls gauge progress.

Update Scoping Parameters
Adjust the scope to encompass new solutions, data flows and interconnections as partnerships grow. Require refreshed information.

Monitor Subcontractors and Acquisitions
Mandate visibility into vendor M&A and subcontracting to evaluate potential new risks requiring updated assessments.

Spot Check Controls
Perform surprise point audits on vendor controls like account permissions and data transfers using your parameters.

Link Performance to Security
Incorporate security criteria into vendor scorecards with penalties for unremediated gaps to drive compliance.

Automate Monitoring Where Possible
Leverage technologies like security ratings services and user behavior analytics for scalable insights into vendor risk profiles and events.

Watch for Red Flags
Investigate changes indicating heightened risk like turnover, regulatory fines, breach disclosures or financial instability. Ongoing vigilance through reviews, audits, monitoring and open communications reinforces the initial foundation laid through rigorous assessments.

TAKE AWAY THOUGHTS

With data breaches rocking major corporations and supply chains, vendor risk management rises as an urgent imperative. Instituting rigorous vendor security assessments provides the visibility required to judge risks before onboarding third parties and enable ongoing oversight.
This guide outlines establishing an effective risk-based assessment program spanning:

- Defining risk categories aligned to your environment
- Collecting comprehensive evidence through questions, documents and interviews
- Objectively evaluating against criteria to identify control gaps
- Quantifying overall vendor risk levels
- Remediating deficiencies through contractual obligations
- Communicating findings to improve security posture
- Maintaining continuous monitoring and reviews

Automation solutions can streamline the process from questionnaires to scoring, while still enabling human validation.

With these core elements in place tailored to your organization, you can expose vendor vulnerabilities before integration and ensure security keeps pace with business expansion. Partners will accept security as a cost of doing business.
While the lifting required on both sides is substantial, vendor assessments represent crucial due diligence. The financial, operational and reputational damage inflicted by a deficient third party is too devastating to neglect this diligence.

In our intricately connected digital economy where companies rely ever more heavily on vendors and partners, ensuring security does not lag is paramount. With a vigorous vendor assessment program empowered by strong criteria, information gathering, analysis, and transparency, organizations can effectively manage risk exposure from third parties.

ETHICO

Contact Us for More Information | 800-859-8840 sales@ethico.com
www.ethico.com