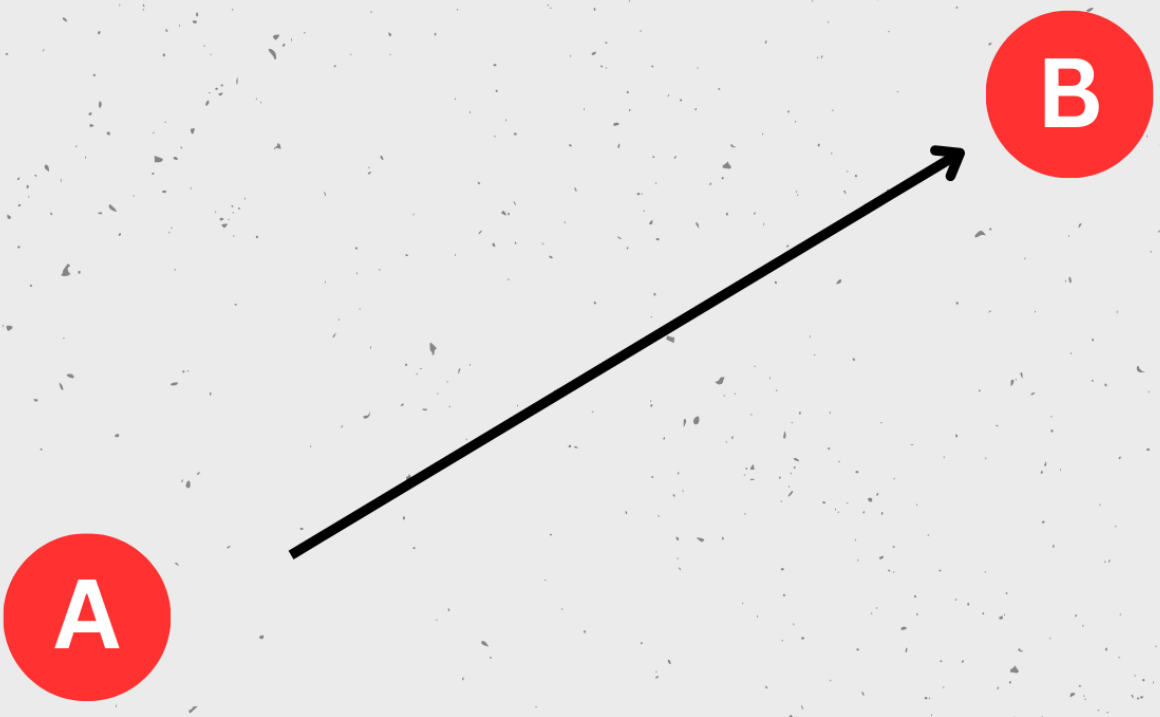
3RD PARTY RISK ASSESSMENT PROGRAM



A ROADMAP TO BUILDING A SUCCESSFUL PROGRAM

SideChannel

Simple 3rd Party Risk Assessment Program

Introduction

Every business relies on outside vendors, whether for cloud services, software, or operational support. While outsourcing brings efficiency and expertise, it also introduces risk. Vendors often handle sensitive company or customer information, making them potential gateways for security incidents. For organizations without a formal cybersecurity program, third-party risk management (TPRM) can feel overwhelming. This guide provides a practical, starting-point approach for evaluating vendors and putting structure around vendor security oversight without requiring a large security team or advanced tools.

Summary

This simple TPRM program helps organizations:

- **Tier vendors by risk** using two easy factors: business value and level of access to data or infrastructure.
- **Apply the right level of oversight**—from asking baseline security questions to requesting certifications, audit reports, or site visits.
- **Leverage vendor resources** such as published compliance pages from major providers (e.g., Microsoft, AWS, Google, Salesforce).
- **Incorporate standard contract protections** like business associate agreements (BAAs), security addendums, or audit rights.
- **Establish a baseline questionnaire** to confirm whether vendors have policies, incident response plans, encryption practices, and security audits in place.

By following these steps, organizations can begin building confidence in their vendor relationships, reduce exposure to external risks, and set the foundation for a stronger cybersecurity program in the future.

Tier vendors by

Compliance Requirements
Y axis - Business Value
X axis - Access Level to Data / Infrastructure

Business Value	**H**	Baseline questions CISO Contact Info	RealCISO Score* Pen Test Attestation Industry Cert Copy CISO Contact Info	RealCISO Score* Pen Test Attestation Industry Cert Copy CISO Contact Info Site Visit
	M	Baseline questions	Baseline questions Industry Cert Copy	RealCISO Score* Pen Test Attestation Industry Cert Copy CISO Contact Info
	L	Baseline questions	Baseline questions Industry Cert Copy	Baseline questions Pen Test Attestation Industry Cert Copy CISO Contact Info
		L	**M**	**H**
		Access Level to Data / Infrastructure		

Note: *The "RealCISO Score" comes from RealCISO, an online platform that provides vendor risk assessments and measures compliance against recognized cybersecurity frameworks. More information is available at https://www.realciso.io/compliance/. This can be substituted for another standard scoring, i.e. maturity, compliance, etc.*

Initial Criteria

When starting vendor risk assessments, the easiest entry point is reviewing what providers already publish. Many major SaaS vendors, like Microsoft, AWS, Google, and Salesforce, maintain detailed compliance pages that outline their certifications, audit reports, and security practices. For new programs, this readily available information serves as a baseline reference without requiring extensive back-and-forth. Organizations can use these compliance resources to quickly validate that key security standards are met and focus their deeper assessments on higher-risk vendors.

Provider	Compliance Page
Microsoft	https://learn.microsoft.com/en-us/compliance/
AWS	https://aws.amazon.com/compliance/programs/
Google	https://cloud.google.com/compliance?hl=en
Salesforce	https://compliance.salesforce.com/en

Security Addendums for Procurement

The security team should provide procurement with standard contract language to ensure vendor agreements include the right protections. At a minimum, this should cover:

- **Business Associate Agreement (BAA) Language** – where applicable, to establish responsibilities for handling sensitive data (e.g., PHI).
- **Technology and Security Amendment** – an addendum requiring the vendor to meet defined security practices, including controls for data protection, breach notification, and audit rights.
- **Core Contract Clauses** – baseline terms that align with the company's risk management program, such as incident response expectations, certification requirements, and right to assess or review security controls.

SideChannel

Baseline questions

1. Do you have a formally appointed information security officer?
    a. If so, please provide the name and contact information.

2. Is your information security program based on an industry accepted framework?
    a. If so, what framework did you choose?

3. Do you have formal information security policies and procedures?
    a. If so, what do your policies address?

4. Have you implemented encryption on all mobile devices and media in which sensitive information is stored (such as, when handling PII, health information, other regulated data or other confidential information on behalf of your customers)?

5. Do you have a formal security incident response plan?
    a. If so, when was the plan last exercised?

6. Do you have a formal disaster recovery plan?
    a. If so, when was the plan last exercised?

7. Have you implemented encryption for all transmission of sensitive/confidential information outside of your organization's network?

8. Have you performed an information security risk assessment within the last year?
    a. If so, was this an internal self-assessment or performed by a third party?
    b. If so, were the results of the assessment remediated to a level accepted by management?
    c. If possible, please share a sanitized executive summary.

9. Do you undergo any industry recognized security audits such as ISO 27001 or SOC2?
    a. If so, please share copies of your report's summary and acceptance by the auditor to include their signature page with contact information.

10. Has your organization experienced any reportable breaches of sensitive/confidential information in the last two years?
    a. If so, provide a summary of the breach and corrective actions taken.

11. Describe how often and what type of security training you provide your employees.

12. Does your product/service support SAML authentication? (N/A is a potential answer)