

7 Steps to a Highly Effective Vendor Risk Management Plan



STEP ONE

Create a Plan and Assign a Team

- Develop a comprehensive Vendor Risk Management Plan.
- Create a Third-Party Vendor Information Security Policy
- Identify key stakeholders throughout the organization to manage the process. (This is not just an IT issue anymore!)



STEP TWO

Identify All of Your Vendors

- Expand the definition of vendor:
 - Networks, components or information systems
 - Physical security and support services
- Create an inventory of your vendor network.
- Determine data access and business criticality



STEP THREE

Tier Vendors Based on Potential Threat

- Tier 1: Business and Mission Critical.
- Tier 2: Access to Highly Sensitive Business and Critical Systems.
- Tier 3: Moderate Access to Networks and Systems.
- Tier 4: Minimal Access to Critical Systems and Networks.



STEP FOUR

Gather Questions for Each Vendor Tier

- Compile a comprehensive list of questions to ask your Tier 1 vendors.
- Tailor questions for lower tiers based on vendor criticality. Take into account the vendor's role and access to systems.
- Meet Regulatory and Compliance requirements.



STEP FIVE

Review Results and Communicate with Vendors

- Score results to clearly identify areas of high risk.
- Address your biggest threats and problems with Tier 1 vendors first.
- Discuss the results with the vendors and communicate proposed solutions or acceptable measures.



STEP SIX

Address any Identified Risks in the Contract Terms and Conditions

- Set minimum standards of conduct and security.
- Institute remediation timelines for security risks. Ensure accountability for breaches.
- Require employee vetting and data access rights management policy. Include clause to audit vendors.



STEP SEVEN

Monitor Your Vendors

- After completing baseline security assessment, the following steps should be part of your plan:
 - Annual Reassessment
 - Real-time critical updates
 - Ad Hoc Vendor Audits (On-site and/or Offsite)

Let Privva Help.

It is no longer enough for a firms to have their internal systems under control; a responsible firm must also monitor and remediate the threat of breach from third-party vendors.

Privva can automate your third-party vendor management making your process faster, easier, and more transparent.

**CONTACT PRIVVA
TO JOIN TODAY.**