10 Essential Steps to Streamline Third-Party Risk Management (TPRM)

APRIL 2020

White Paper/Guide

OneTrust Vendorpedia™
THIRD-PARTY RISK SOFTWARE

10

Essential Steps to Streamline Third-Party Risk Management (TPRM)

Third-party risk management (TPRM) isn't a new concept, however, recent events have brought the discipline into the forefront like never before. Organizations in all industries rely on third parties, whether they be cloud service providers, suppliers, contractors, and other vendors.

Crucially, when the supply chain is interrupted, or third parties can't deliver, there can be devastating and long-lasting impacts. In this short whitepaper, we'll outline 10 essential steps that organizations can take to build a streamlined TPRM program.

PHASE TWO: BUILD THE FOUNDATION

3. Choose Your Standard or Framework

The standard that makes sense for your organization is completely dependent on your internal risk program, as well as industry, region, and other contributing factors. Many organizations will select a standard, and then customize it to meet their requirements. Some of the most common standards and frameworks used to assess third parties are:

SFG SHARED ASSESSMENTS The Trusted Source in Third Party Risk Management

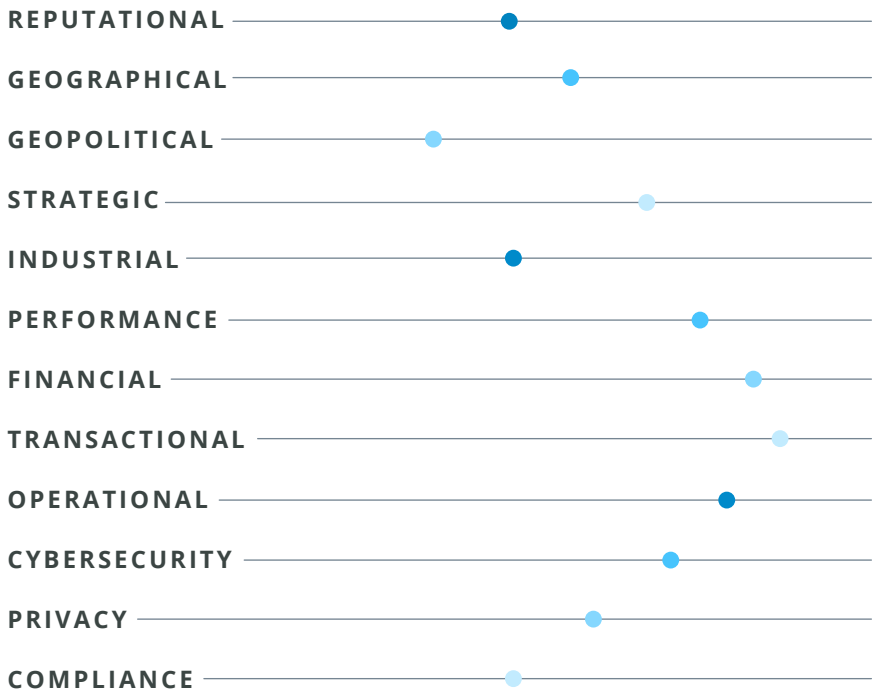
ISO

NIST

CSA cloud security alliance®

4. Understand the Risks You Care About

There are many different types of risks to consider when building your TPRM program. Companies will often classify risks to better report on the potential threats posed by a vendor. Common risk classifications include:



PHASE THREE: BUILD YOUR INVENTORY

5. Know Your Third Parties

There are several ways to discover which third parties your organization works with. This process can take time, however there are tactics you can use to streamline the process.

Use Existing Information

Many organizations maintain their list of service providers in a spreadsheet or database; however, these lists are often disorganized, out-of-date, and incomplete. Still, we can use this information as a starting point by bulk importing it into a central inventory.

Leverage DataDiscovery to Identify Third-Party Technologies

Identify the existing service providers in use by looking to existing technologies, such as CMDBs, SSO providers, contract, procurement, and other tools to pull in and centralize all information relating to service providers.

Conduct Assessments or Interviews

Conduct internal assessments and interviews to identify the third parties in use. Many organizations will send a short assessment to business owners across the company, such as marketing, HR, finance, sales, research and development, and other departments. These business leaders can provide valuable details on the tools in use across your organization.

Leverage Self-Service Portals

With a self-service portal, you can enable the business to help build your inventory. Link to the portal within your intranet or SharePoint for easy access, and use a short threshold assessment to identify vendors and gather preliminary information about the third party, such as:

- Vendor Name
- Expexted procurement date
- Business purpose
- Primary vendor contact (email, phone, address)
- Data type involved
- Prior security reviews or certifications, if applicable
- Personal information involved
- Hosting information
- Privacy Shield and other certification
- Business context
- Scope of engagement

6. Classify Your Third Parties

Classifying vendors helps streamline your TPRM program by enabling you to direct your focus to the third parties that present the most risks. To classify third parties, companies often determine the inherent risk of their vendors. To determine inherent risks, organizations will send a quick questionnaire to understand details, such as:

- Service provided
- Access to data
- Data type/sensitivity
- Security and privacy expectations
- Financial standing of the vendor
- Value of contract
- Prior engagements with vendor
- Data transfers
- Location (of operation & data storage)
- Strategic value to your business
- Length of relationship

Using inherent risk, TPRM teams can bucket vendors into tiers, with tier one vendors usually designated as the most critical.

PHASE FOUR: STREAMLINE ASSESSMENTS & DUE DILIGENCE

7. Perform Assessments and Mitigate Risks

Assessments take time and are resource intensive. Instead of sending a detailed assessment via a spreadsheet, many TPRM programs are taking advantage of new trends in the market, such as:

- Pre-completed assessments made available through a Cyber Risk Exchange
- Vendor chasing services to order assessments as a service
- Assessment automation technology to streamline questionnaire completion

If you opt to perform the assessment yourself, one of the primary goals is to understand what controls a vendor has in place. When critical controls (or the lack thereof) are identified), risks can be calculated, and mitigation can begin. Common risk mitigation workflows include:

IDENTIFICATION
At this stage, risks are flagged and given a risk level or score.

EVALUATION
During the valuation phase, organizations will determine if the risk appetite.

TREATMENT
When treatment occurs, a risk owner must validate that the required controls are in place to reduce the risk to the desired residual risk level.

MONITORING
At this phase, organizations monitor risks for any events that may increase the risk level, such as a data breach.

8. Manage Key Contract Terms

Contracts are often long and extremely detailed, with some aspects falling outside the realm of TPRM. Still, there are key provisions, clauses, and terms that TPRM teams should look out for when reviewing vendor contracts. Some of these include:

- Defined Scope of Services or Products
- Price and Payment Terms
- Term and Termination Clauses
- Intellectual Property Ownership Clause
- Deliverables or Services Clause
- Representation and Warranties
- Confidentiality Clause
- Disclaimers or Indemnification
- Limitation of Liability
- Insurance
- Relationship Clause
- Data Processing Agreement
- 4th Party or Subprocessor Change Clauses
- Compliance Clause
- Data Protection Agreement
- Service Level Agreements (SLAs), Product Performance, Response Times

Many TPRM professionals will extract key terms in a structured format to determine if key contractual clauses are adequate, inadequate, or missing. This "structured" and simplified tracking method makes executive-level reporting possible and offers clarity when it comes to contracts.

PHASE FIVE: MAINTAIN AND MONITOR

9. Generate Reports and Maintain Records for Compliance

To build a defensible and audit-ready TPRM program, organizations must maintain records for demonstrating compliance. This step is often overlooked – until audits occur – and is one of the most significant aspects of a well-oiled TPRM program. Maintaining these records in spreadsheets is nearly impossible at scale. Purpose-built TPRM software can automate recordkeeping and leave you with detailed activity trails to simplify audits.

With detailed records maintained, it becomes much easier to report on the things that matter most to your organization. In practice, we see organizations create dashboards that show:

- Total supplier count
- Suppliers sorted by risk level
- Status on all supplier risk assessments
- Number of suppliers with expiring or expired contracts
- Risks grouped by level (high, medium, low)
- Risks by stage within the risk mitigation workflow
- Risks to your parent organization and risks to your subsidiaries
- Risk history over time

10. Monitor Vendor, Market, and Regulatory Changes Over Time

TPRM is far from a static discipline. With new regulations, emerging threats, high-profile data breaches, and evolving standards, organizations have their work cut out for them – which is why the industry is pushing for ongoing third-party risk monitoring. Assessments offer "moment-in-time" glimpses of a vendor's risk posture, however, risks can drastically change at any time. Beyond cybersecurity, significant risk-changing events to monitor include:

- Mergers, acquisitions, or divestitures
- Internal process changes
- Negative news or unethical behavior
- Natural disasters and other business continuity triggering events
- Product releases
- Contract changes
- Industry or regulatory developments
- Financial viability or cash flow
- Employee reduction
- And much more...

If you don't have a tool in place to constantly monitor your vendors, consider re-evaluating your vendors on regular schedule. This schedule may be determined based on the inherent or residual risk of the third party, on a time-based schedule, or when contracts are up for renewal.

Want to see how **OneTrust Vendorpedia** can help you mature and manage your third-party risk program? ***Request a demo today.***

OneTrust Vendorpedia™

THIRD-PARTY RISK SOFTWARE

About Vendorpedia

OneTrust Vendorpedia™ is the largest and most widely used technology platform to operationalize third-party risk, security, and privacy management. More than 5,000 customers of all sizes use OneTrust, which is powered by 75 awarded patents, to offer the most depth and breadth of any third party risk, security, and privacy solution in the market. OneTrust Vendorpedia is purpose-built software designed to help organizations manage vendor relationships with confidence and integrates seamlessly with the entire OneTrust platform, including OneTrust Privacy, OneTrust GRC, OneTrust DataGuidance™, and OneTrust PreferenceChoice™.

Backed and co-chaired by the founders of Manhattan Associates (NASDAQ: MANH) and AirWatch ($1.54B acq. by VMware), and supported by a $200 million Series A funding from Insight Partners, the OneTrust leadership team has significant experience building scalable, enterprise software platforms. OneTrust is also guided by an external advisory board of renowned privacy experts and an in-house global privacy and legal research team. OneTrust is co-headquartered in Atlanta and in London, and has additional offices Bangalore, San Francisco, Melbourne, New York, São Paulo, Munich, Hong Kong, Bangkok.

To learn more, visit **Vendorpedia.com** or connect on **LinkedIn**.