**Third-Party Risk Management**

Third-party risk management (TPRM) is a form of risk management that focuses on identifying and reducing risks relating to the use of third parties (sometimes referred to as vendors, suppliers, partners, contractors, or service providers).

The discipline is designed to give organizations an understanding of the third parties they use, how they use them, and what safeguards their third parties have in place. The scope and requirements of a TPRM program are dependent on the organization and can vary widely depending on industry, regulatory guidance, and other factors. Still, many TPRM best practices are universal and applicable to every business or organization.

While exact definitions may vary, the term “third-party risk management” is sometimes used interchangeably with other common industry terms, such as  [vendor risk management](https://www.onetrust.com/blog/vendor-risk-management/) (VRM), vendor management, supplier risk management, or supply chain risk management. However, TPRM is often thought of as the overarching discipline that encompasses all types of third parties and all types of risks.

**Why is Third-Party Risk Management Important?**

While third-party risk isn’t a new concept, upticks in breaches across industries and a greater reliance on outsourcing have brought the discipline into the forefront like never before. Disruptive events, have impacted almost every business and their third parties – no matter the size, location, or industry. In addition, data breaches or cyber security incidents are common. In in 2021, the impact that third parties have on business resilience was highlighted through outages and other third-party incidents. Some of the ways you can be impacted are:

* Internal outages and lapses in operational capabilities
* External outages affecting areas across the supply chain
* Vendor outages that open your organization to supply chain vulnerabilities
* Operational shifts that affect data gathering, storage, and security

Most modern organizations rely on third parties to keep operations running smoothly. So, when your third parties, vendors, or suppliers can’t deliver, there can be devastating and long-lasting impacts.

For example, you may rely on a service provider such as Amazon Web Services (AWS) to host a website or cloud application. Should AWS go offline, your website or application also goes offline. An additional example could be the reliance on a third party to ship goods. If the shipping company’s drivers go on strike, that can delay expected delivery times and lead to customer cancellations and distrust, which will negatively impact your organization’s bottom line and reputation.

Outsourcing is a necessary component of running a modern business. It not only saves a business money, but it’s a simple way to take advantage of expertise that an organization might not have in house. The downside is that if a proper TPRM program is not in place, relying on third parties can leave your business vulnerable.

**What are the Top TPRM Best Practices?**

There are endless TPRM best practices that can help you build a better program, regardless of whether you’re just beginning to make TPRM a priority, or you want to understand where your existing program could be improved.

We’ve outlined what we believe are the 3 most critical best practices that are applicable to nearly every company.

1) **Prioritize Your Vendor Inventory**

Not all vendors are equally important, which is why it is critical to determine which third parties matter most. To improve efficiency in your TPRM program, segment your vendors into criticality tiers.

Most companies segment vendors into three groups:

* **Tier 3:** Low risk, low criticality
* **Tier 2:** Medium risk, medium criticality
* **Tier 1:** High risk, high criticality

In practice, organizations will focus their time and resources on tier 1 vendors first, as they require more stringent due diligence and evidence collection. Typically, tier 1 vendors are subject to the most in-depth assessments, which often includes on-site assessment validation.

Many times, especially during initial evaluation, these tiers are calculated based on the inherent risk of the third party. Inherent risk scores are generated based on industry benchmarks or basic business context, such as whether or not you will be:

* Sharing proprietary or confidential business information with the vendor​
* Sharing personal data with the vendor​
* Sharing *sensitive* personal data with the vendor​
* Sharing personal data across borders​
* Serving a critical business functions​

Additionally, impact of the vendor can be a determining factor. If a third party can’t deliver their service, how would that impact your operations? When there is significant disruption, the risk of the vendor will inevitably be higher. Determine this impact by considering:

* The impact of unauthorized disclosure of information​
* The impact of unauthorized modification or destruction of information​
* The impact of disruption of access to the vendor/information​

Another way to tier vendors is by grouping based on contract value. Big-budget vendors may automatically be segmented as a tier 1 vendor due to the high risk based solely on the value of the contract.

**2) Leverage Automation Wherever Possible**

Efficiencies emerge when operations are consistent and repeatable. There are a number of areas in the TPRM lifecycle where automation is ideal. These areas include, but are not limited to:

* **Intaking and**[**onboarding new vendors**](https://www.onetrust.com/products/third-party-risk-management/)**.**  Automatically add vendors to your inventory using an intake form or via integration with contract management or other systems.
* **Calculating inherent risk and tiering vendors.** During intake, collect basic business context to determine a vendor’s inherent risk, and then automatically prioritize vendors posing the highest risk.
* **Assigning risk owners and mitigation tasks.** When a vendor risk is flagged, route the risk to the correct individual and include a checklist of mitigation action items.
* **Triggering vendor performance reviews.** Set up automation triggers to conduct a review of the vendor each year, and if the vendor fails the review, trigger off-boarding actions.
* **Triggering vendor reassessment.** Send a reassessment based on contract expiration dates and save the previous year’s assessment answers so the vendor doesn’t have to start from scratch.
* **Sending notifications and other alerts.** When a new risk is flagged or a new vendor is onboarded, send an email or alert the relevant stakeholder through an integration with an existing system.
* **Scheduling and running reports.** Set up automated reports that run on a daily, weekly, or monthly basis and automatically share them with the right person.

Every TPRM program is different, so start by looking internally at the repeatable processes that are ripe for automation. From there, start small and take practical steps to automate key tasks. Over time, these small automations will compound, saving your team valuable time, money, and resources.

**3) Think Beyond Cybersecurity Risks**

When considering a third-party risk or vendor risk management program, many organizations immediately think aboutcybersecurity risks. But TPRM entails so much more. While starting small and focusing only on cybersecurity risks is a good first step, there are other types of risks that need to be prioritized. These risks include:

* Reputational risks
* Geographical risks
* Geopolitical risks
* Strategic risks
* Financial risks
* Operational risks
* Privacy risks
* Compliance risks
* Ethical risks
* Business continuity risks
* Performance risks
* 4th party risks
* Credit risks
* Environmental risks

The key takeaway here is that understanding all relevant types of risk (and not just cybersecurity) is imperative to building a world-class TPRM program.

**Third-Party Risk Management Lifecycle**

The third-party risk management lifecycle is a series of steps that outlines a typical relationship with a third party. TPRM is sometimes referred to as “third-party relationship management.” This term better articulates the ongoing nature of vendor engagements. Typically, the [TPRM lifecycle](https://www.onetrust.com/blog/tprm-lifecycle/), is broken down into several stages. These stages include:

1. [Vendor identification](https://www.onetrust.com/blog/third-party-risk-management/#vendor-identification)
2. [Evaluation & selection](https://www.onetrust.com/blog/third-party-risk-management/#evaluation)
3. [Risk assessment](https://www.onetrust.com/blog/third-party-risk-management/#risk-assessment)
4. [Risk mitigation](https://www.onetrust.com/blog/third-party-risk-management/#risk-mitigation)
5. [Contracting and procurement](https://www.onetrust.com/blog/third-party-risk-management/#contracting-and-procurement)
6. [Reporting and Record-keeping](https://www.onetrust.com/blog/third-party-risk-management/#reporting-and-recordkeeping)
7. [Ongoing monitoring](https://www.onetrust.com/blog/third-party-risk-management/#ongoing-monitoring)
8. [Vendor off-boarding](https://www.onetrust.com/blog/third-party-risk-management/#vendor-management)

**Phase 1: Third-Party Identification**

There are many ways to identify the third parties your organization is currently working with, as well as ways to identify new third parties your organization wants to use.

To identify vendors already in use and build a vendor inventory, organizations take multiple approaches, which include:

* Using existing information. Organizations often consolidate vendor information from spreadsheets and other sources when rolling out third-party risk software.
* Integrating with existing technologies. Technologies that are in use often contain detailed vendor information, such as CMDBs, SSO providers, contracts, procurement, and other systems. Organizations will often plug into these sources to centralize their inventory in a single software solution.
* Conducting assessments or interviews. A short assessment to business owners across the company, such as marketing, HR, finance, sales, research and development, and other departments can help you uncover the tools in use at your organization.

To identify new third parties, organizations will often leverage a self-service portal as part of their third-party risk management program. With a self-service portal, business owners can build their inventory. Share the portal with your business by linking to it from your intranet or SharePoint. Self-service portals also help gather preliminary information about the third party, such as:

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

Using this information, you can classify third parties based on the inherent risk that they pose to your organization.

**Phase 2: Evaluation and Selection**

During the evaluation and selection phase, organizations consider RFPs and choose the vendor they want to use. This decision is made using a number of factors that are unique to the business and its specific needs.

**Phase 3: Risk Assessment**

Vendor risk assessments take time and are resource-intensive, which is why many organizations are using a [third-party risk exchange](https://www.onetrust.com/products/third-party-risk-exchange/) to access pre-completed assessments. Other common methods include using spreadsheets or assessment automation software. Either way, the primary goal of understanding the risks associated with the vendor is the same.

Common standards used for assessing vendors include:

* [ISO 27001](https://www.onetrust.com/products/third-party-risk-management/) & [ISO 27701](https://www.onetrust.com/solutions/iso27701-compliance/)
* [SIG Lite & SIG Core](https://www.onetrust.com/products/third-party-risk-management/)
* [NIST SP 800-53](https://www.onetrust.com/products/third-party-risk-management/)
* [CSA CAIQ](https://www.onetrust.com/products/third-party-risk-management/)

As well as industry-specific standards, such as:

* [HITRUST](https://hitrustalliance.net/)
* [HECVAT](https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit)

**Phase 4: Risk Mitigation**

After conducting an assessment, risks can be calculated, and mitigation can begin. Common risk mitigation workflows include the following stages:

* At this stage, risks are flagged and given a risk level or score.
* During the evaluation phase, organizations will determine if the risk is acceptable within their defined risk appetite.
* 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.
* At this phase, organizations monitor risks for any events that may increase the risk level, such as a data breach

**Phase 5: Contracting and Procurement**

Sometimes done in parallel with risk mitigation, the contracting and procurement stage is critical from a third-party risk perspective. Contracts often contain details that fall 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 Time

Home in on these key terms to report on requirements in a structured format. Simply determine if key clauses are adequate, inadequate, or missing.

**Phase 6: Reporting and Recordkeeping**

Building a strong TPRM program requires organizations to maintain compliance. This step is often overlooked. Maintaining detailed records in spreadsheets is nearly impossible at scale, which is why many organizations implement TPRM software. With auditable recordkeeping in place, it becomes much easier to report on critical aspects of your program to identify areas for improvement.

In practice, a sample reporting dashboard may include:

* 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

**Phase 7: Ongoing Monitoring**

An assessment is a “moment-in-time” look into a vendor’s risks; however, engagements with third parties do not end there – or even after risk mitigation. Ongoing vendor monitoring throughout the life of a third-party relationship is critical, as is adapting when new issues arise.

For example, new regulations, negative news stories, high-profile data breaches, and evolving usage of a vendor, may all impact the risks associated with your third parties. Some key 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

**Phase 8: Vendor Offboarding**

A thorough offboarding procedure is critical, both for security purposes and recordkeeping requirements. Many organizations have developed an offboarding checklist for vendors, which can consist of both an assessment sent internally and externally to confirm that all appropriate measures were taken. Critical too is the ability to maintain detailed evidence trail of these activities to demonstrate compliance in the event of regulatory inquiry or audit.

**Which Department Owns TPRM?**

There is no one-size-fits-all approach to third-party risk management. All companies are different, and as a result, there is no set-in-stone department that owns vendor risk responsibilities. Some mature organizations may have a third-party risk or vendor management team, but many organizations do not. As a result, common job titles and departments that “own” third-party risk include:

* Chief Information Security Officer (CISO)
* Chief Procurement Officer (CPO)
* Chief Information Officer (CIO)
* Chief Privacy Officer (CPO)
* Information Technology (IT)
* Sourcing and Procurement
* Information Security
* Risk and Compliance
* Supply Chain Manager
* Third-Party Risk Manager
* Vendor Risk Manager
* Vendor Management
* Contract Manager

The list above is by no means comprehensive; however, the diverse variety of titles and departments can shed some light on the diverse approaches taken to third-party risk management.

Ultimately, these stakeholders and departments must work together to manage vendors throughout the [third-party lifecycle.](https://www.onetrust.com/blog/tprm-lifecycle/) As such, TPRM often extends into many departments and across many different roles.

**What are the Benefits of Third-Party Risk Management Software?**

With [third-party risk software](https://www.onetrust.com/products/third-party-risk-management/), your organization can develop and scale a successful TPRM management program that adds value to your bottom line. The return on investment (ROI) is significant when leveraging the automation opportunities that purpose-built software provides. The biggest benefits include:

* Improved security
* Improved customer trust
* Increased time savings
* Increased cost savings
* Less redundant work
* Better data visibility
* Faster vendor onboarding
* Simpler assessments
* Better reporting capabilities
* Easier audits
* Less risks
* Better vendor performance
* Less spreadsheets