What is Third-Party Risk Management

June 1, 2021 - Third Party Risk

What is 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 third-party risk management 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 (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, recent events and a greater reliance on outsourcing have brought the discipline into the forefront like never before. Disruptive events, such as the COVID-19 pandemic, 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 fact, more than half of the breaches that have occurred over the past two years were caused by a third party.

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.

- 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 third-party risk management lifecycle where automation is ideal. These areas include, but are not limited to:

- **Intaking and onboarding new vendors.** 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

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
- And many more…

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

What is the 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, is broken down into several stages. These stages include:

1. Vendor identification
2. Evaluation & selection
3. Risk assessment
4. Risk mitigation
5. Contracting and procurement
6. Reporting and Recordkeeping
7. Ongoing monitoring

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 vendors 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 which 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 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& ISO 27701
- SIG Lite & SIG Core
- NIST SP 800-53
- CSA CAIQ

As well as industry-specific standards, such as:

- HITRUST

- 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

Hone 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 or VRM 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

- 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. While some mature organization 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. As such, TPRM often extends into many departments and across many different roles.

- Easier audits
- Less risks
- Better vendor performance
- Less spreadsheets
- And much more...

Want to see how OneTrust Vendorpedia can help your organization streamline third-party risk management? Request a demo today!

Share this Article

Related Posts

The CPO & Vendor Risk Management: Top Challenges & Biggest Opportunities

As the privacy landscape continues to evolve, key focus areas of privacy program management are shifting. A product of

The CISO & Vendor Risk Management: Top Challenges & Biggest Opportunities

As security teams spent the last year adapting to rapid digital transformation, the quick expansion left them spread thin, exposing new vulnerabilities for bad actors

Risk Management: Making Your Organization First Line Friendly

What does it mean to make your risk management program first line friendly? While risk management is critical to an organization's

RFP Template

Incident & Breach Response
View All Products

Services

Professional Services
Training & Certification
Partners

Publishers & Advertisers
Risk, Compliance & Audit

Large Enterprises
Small & Mid-Size Companies

GDPR | CCPA | LGPD
View All Laws & Frameworks

Blog
Integrations Marketplace
PrivacyConnect Workshops
PrivacyTech User Groups
View All Resources

Awards
Trust
Contact Us

Get in Touch

info@onetrust.com
+1 (844) 847-7154

support@onetrust.com
myOneTrust Portal

Be in the Know

Subscribe to our newsletter

What's your email address?

Subscribe

Privacy Matters

Our privacy center makes it easy to see how we collect and use your information.

Your Privacy

When we collect your personal information, we always inform you of your rights and make it easy for you to exercise them. Where possible, we also let you manage your preferences about how much information you choose to share with us, or our partners.

Our Policies

Read our Privacy Notice and Cookie Notice.

Visit our Trust page and read our Transparency Report.

Your Rights

Exercise Your Rights. Let us know how we can help.

Do Not Sell My Personal Information

Customize Settings

Disable All

Allow All