What Is the Third-Party Risk Management Lifecycle?

WHY YOU NEED IT

Various industry regulators such as the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), U.S. Department of Health and Human Services (HHS) and National Credit Union Association (NCUA) set the standards for managing third-party vendor relationships.

These agencies often look to one another for best practices and have similar expectations.

Though processes and procedures can vary by industry and organization, the evolving third-party risk management (TPRM) best practices have been shaped by regulatory requirements.

Regulatory compliance can be achieved by following the practices outlined in the TPRM lifecycle.

LAYING THE LIFECYCLE FOUNDATION

Three fundamental elements create the foundation of the TPRM lifecycle:

Oversight and Accountability

Typically, an organization's board of directors or senior management team will determine the oversight and accountability roles which are then formalized and communicated through official governing documents.

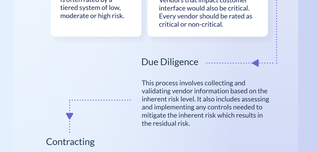
Documentation and Reporting

Well-written governance documents are essential to a TPRM lifecycle (e.g., policy, program and procedures). Reporting requirements should be defined in policy and program materials regularly provided to appropriate stakeholders.

Independent Review

There's always room for improvement when it comes to the TPRM lifecycle. Independent audit and third-party assessors should be treated as valuable assets that test your program and provide valuable feedback to help ensure that you're meeting regulatory guidance.

Each in-scope vendor that provides products or services to your organization should progress through the following TPRM lifecycle stages:



Onboarding

Introducing a new vendor into your organization requires a lot of planning and consideration. Before signing the contract, you must begin the onboarding process with a thorough assessment of a vendor's inherent risk and criticality. You can then use this information to conduct risk-based due diligence and decide whether to proceed with contracting.

Here's a quick overview of what's included in onboarding:

Planning & Risk Assessment

Before you begin onboarding, you'll need to establish a clearly defined scope for what must go through the TPRM lifecycle. You can generally exclude customers, clients and business partners, but make sure to create a repeatable process to define what a vendor, service provider or third party is to your organization.

You'll also need to determine the inherent risk and criticality during the risk assessment:

Inherent risk is a natural part of the product or service and serves as the relationship default.

This is assessed without considering any existing or future precautions or controls. Inherent risk is often rated by a tiered system of low, moderate or high risk.

Criticality refers to the business impact on your organization if the vendor fails or goes out of business.

Critical vendor engagements can include products and services necessary to sustain your core operations or comply with regulatory requirements. Vendors that impact customer interface would also be critical. Every vendor should be rated as critical or non-critical.

Due Diligence

This process involves collecting and validating vendor information based on the inherent risk level. It also includes assessing and implementing any controls needed to mitigate the inherent risk which results in the residual risk.

Contracting

After deciding if the residual risk is acceptable, you can then formally select the vendor and manage the contract.

This process includes internal planning, negotiating, creating/drafting, approving/executing, storing and managing of the vendor contract. Service level agreements (SLAs) are also an important component to keep both parties accountable.

Ongoing

Stay aware of any new or emerging risks by maintaining a practice of ongoing monitoring and periodic re-evaluations or vendor information.

The TPRM lifecycle should include the following activities on a recurring basis:

Re-Assessments

Risk should be assessed periodically depending on the level of inherent risk. A good standard is to re-assess critical and high-risk vendors at least annually, moderate-risk vendors every 18 months to two years and low-risk vendors every two to three years.

Monitoring & Performance

Ongoing monitoring of risk and performance ensures that quality and risk level stay consistent and acceptable throughout the relationship. Contractual SLAs are needed when monitoring the vendor's performance. These performance metrics allows you to spot trends and prepares you to remediate any issues when they arise.

Renewals

Contract renewals require careful planning to allow for any negotiations or changes you may need to implement. Review the contract well before the renewal period as negotiating any changes can be a time-consuming process.

Due Diligence

Recurring due diligence is an important practice in the event of a pending contract renewal, decline in vendor performance or updated regulatory requirements.

Offboarding

Finally, there comes a time when an engagement must come to an end. Maybe because a vendor failed to perform, the contracted term ended or you just need to move on to bigger and better things. Whatever the reason, there should always be some consideration of the termination process for any vendor.

A well-planned offboarding strategy will include the following activities:

Termination

This is the step in which you notify the vendor that the contract won't be renewed after it expires. Keep in mind that the vendor engagement won't be officially terminated until the date stated on the contract.

Exit Plan Execution

Follow your exit plan to ensure both parties have a smooth transition when offboarding. You'll want to ensure that the vendor completes their responsibilities such as returning or disposing of your organization's data.

At the same time, your organization will perform its duties, which might include revoking all vendor access to your systems and facilities, transitioning to another vendor or bringing the activity in-house.

TPRM Closure

After completing the exit plan, there may be a few final steps to formalize the closure of the relationship. This might include reviewing and paying any final invoices and working with accounts payable to prevent payment of any future invoices.

All relevant vendor information should be appropriately filed or archived should you need access to it later (perhaps for an audit).

The third-party risk management lifecycle is a valuable practice that satisfies regulators and protects your organization from vendor risk when followed consistently.

Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

DOWNLOAD NOW

PRINTABLE VERSION

Copyright © 2022 by Venminder, Inc.

venminder

Manage Vendors. Mitigate Risk. Reduce Workload.

+1 (866) 836-6463 | venminder.com