The Third-Party Risk Management Lifecycle

venminder

STAGE 1
Onboarding

You need to fully understand the amount and types of risk that your organization will have to manage way before you get to the point of selecting a vendor and signing the contract.

Planning & Risk Assessment

Establish a clearly defined scope and repeatable process for what needs to go through the third-party risk management (TPRM) lifecycle. Customers, clients and business partners will generally be excluded from this process.

Inherent risk *naturally occurs as part of the product or service (and is the relationship default). It's assessed without considering any existing or future precautions or controls and is often rated on a scale of low, moderate or high.*

Criticality *reflects the business impact on your organization should the vendor fail or go out of business. Critical vendors typically provide products or services necessary to sustain your core operations or meet regulatory compliance. Every vendor should be rated as critical or non-critical.*

Due Diligence

Once you've determined the vendor's inherent risk level and criticality, you can proceed to risk-based due diligence. This process involves collecting and validating information from and about the vendor. You can then evaluate or implement controls to mitigate or reduce the inherent risk.

Contracting

A well-written contract is essential. It can protect your organization against unexpected problems and will also help save time and money.

STAGE 2
Ongoing

Maintain a healthy routine of ongoing monitoring throughout the vendor relationship so you can remain aware of any new or evolving risks.

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 vendors every 18 months to two years and low-risk vendors every two to three years.

Monitoring & Performance

A vendor's risk and performance should be regularly monitored throughout the engagement to ensure both remain consistent. By monitoring contractual service level agreements, you can spot trends and be better prepared to fix any issues.

Renewals

Contract renewals require strategic planning to ensure that you have sufficient time for potential negotiations. Reviewing the contract well ahead of the scheduled renewal allows you to maintain a successful vendor partnership.

Due Diligence

Collecting and reviewing vendor due diligence should be recurring, based on pending contract renewal, updated regulatory requirements or performance issues.

STAGE 3
Offboarding

Some vendor engagement must come to an end. This can occur for various reasons, from a decline in performance to increasing prices. Regardless of the reason, you must establish an effective offboarding process that minimizes business disruption.

Termination

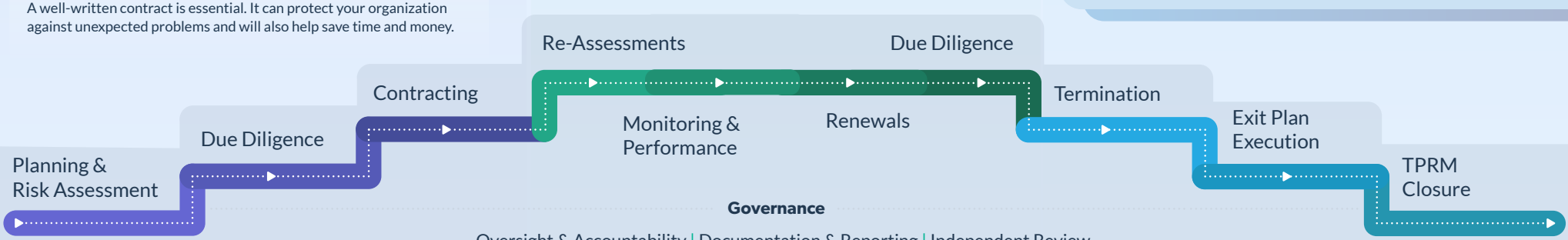
This refers to the task of notifying the vendor that the contract won't be renewed after its expiration.

Exit Plan Execution

Following the steps in your exit plan will help create a smooth transition for both parties. Ensure that the vendor completes their final tasks such as returning or disposing your sensitive data. Your organization will also need to fulfill its duties of removing the vendor from your inventory.

TPRM Closure

Final closure of the TPRM program may include any required steps to recognize that the vendor is no longer active. Vendor information may still be on file but moved to an archived status.



ALWAYS OCCURRING
Governance

Oversight and Accountability
These roles are typically determined by the board of directors or senior management and formalized and communicated through official governing documents.

Documentation and Reporting
Governance documents typically include a policy, program and procedures. These communicate TPRM roles and responsibilities and set expectations for reporting that are timely and accurate.

Independent Review
Independent audits and third-party assessments can help ensure your program is tested and meets regulatory requirements.