Guidance on How to Master Third-Party Risk Management in 2023

venminder

Guidance on How to Master Third-Party Risk Management in 2023

The success of a third-party risk management program depends on a carefully integrated combination of rules, tools, processes, and people. With so many interdependent components, it can be difficult to know exactly where your program is and how to take it to the next level. **If you're struggling to figure it out, there's good news: there's already a well-established roadmap.** You can follow the third-party/vendor risk management lifecycle, which was specifically designed to help you identify, assess, manage, and monitor vendor risk in your organization.

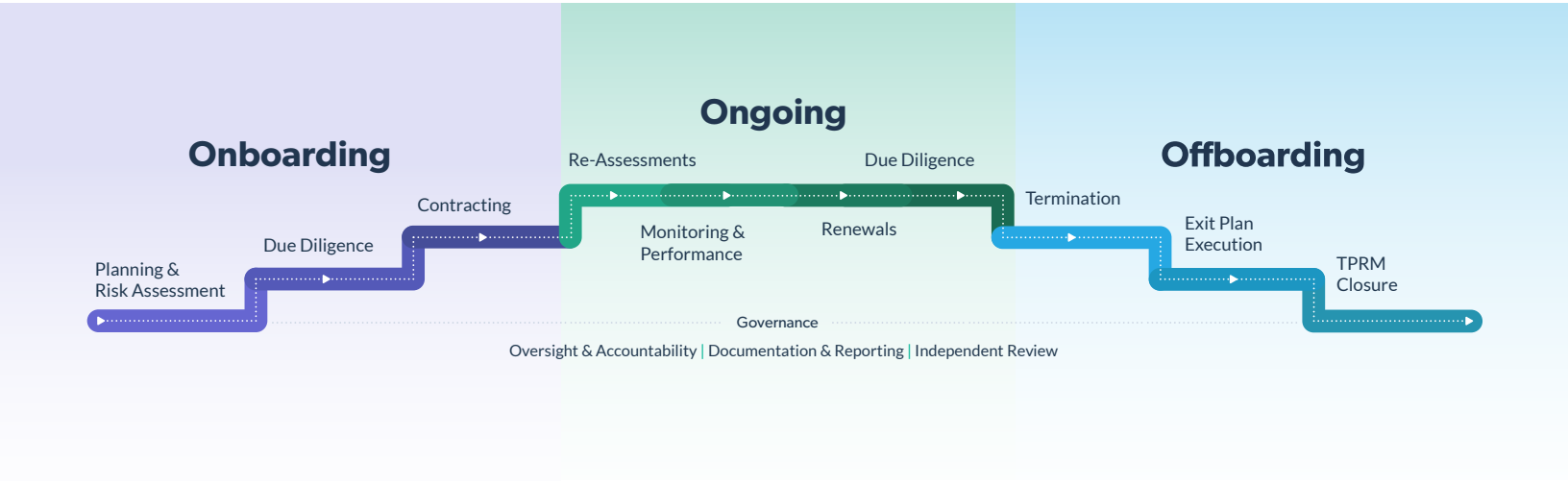
This eBook will examine the third-party/vendor risk management lifecycle in detail. We'll cover each of its three stages as well as the activities you should complete along the way. You'll also find helpful guidance and information to consider, professional tips, and some common mistakes to avoid. If you're interested in mastering third-party risk management, read on to learn more.

Introduction to the Third-Party (Vendor) Risk Management Lifecycle

The third-party (or vendor) risk management lifecycle is the foundation of an effective third-party risk management program. While financial regulators originally envisioned the lifecycle, it has since evolved to become the best practice for all third-party or vendor risk management programs, regardless of industry type or organization.

The lifecycle serves as a roadmap for every vendor relationship. Organizations can use the lifecycle as a guide for identifying, assessing, managing, and mitigating vendor risks from the relationship's beginning until the relationship's end and everything in between.

> **The lifecycle has three distinct stages:** onboarding, ongoing, and offboarding, and is **supported by a strong foundation** of oversight and accountability, documentation and reporting, and independent review.
>
> There are multiple activities and processes involved in the lifecycle, which follow a set sequence. Following the order of activities is important to ensure the most comprehensive risk identification, assessment, and management throughout the vendor relationship.



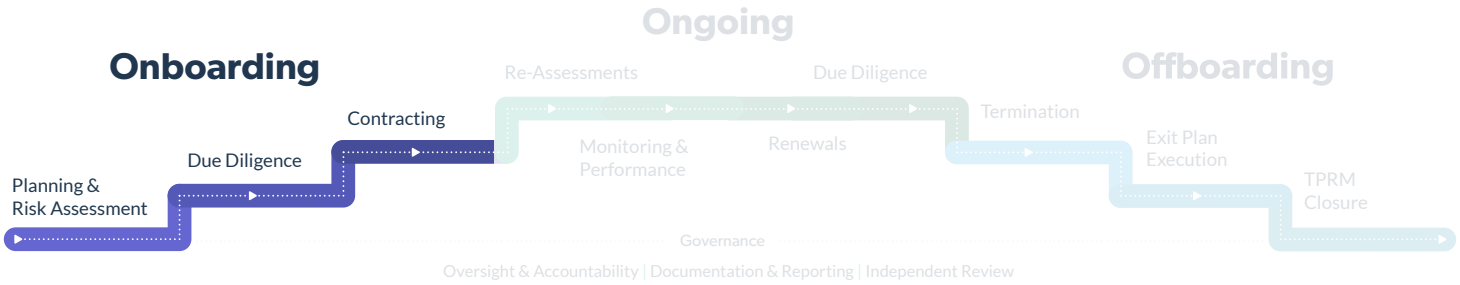
The 3 Stages of the Vendor Risk Lifecycle

Onboarding

The first stage of the lifecycle is onboarding, which incorporates all the steps and activities that must occur up until the contract is signed and executed. To begin this stage, you must plan for the relationship by determining if the vendor type (product or service) is in scope for your third-party risk management program and identify who will be responsible for the day-to-day vendor management.

There are risks that naturally occur with every product or service, called inherent risks. At the onboarding stage, one of the most important aspects is identifying the inherent risks associated with the product, service, or vendor relationship. It's also essential to determine whether the product or service will be critical to your operations.

Once your inherent risk assessment is complete, you should know your vendor's risk level or rating as well as their criticality. This information is the foundation for how you'll treat and manage the vendor throughout the relationship.



Then, it is time to perform due diligence. Due diligence is the process of reviewing your vendor's reputation, determining whether they're a legitimate business entity, and ensuring that the vendor has the appropriate controls to manage the identified risks.

At the completion of due diligence, you'll be able to determine if your organization should proceed with the relationship. If so, contract negotiation and execution can take place.

Let's explore each of these activities and processes in more detail.

Who's In Scope for Third-Party/Vendor Risk Management?

It's common to describe businesses and individuals that provide products or services directly to an organization as "third parties" or "vendors." However, not every third party or vendor may be in scope for your program.

Before bringing a vendor into your organization, you must determine if the potential vendor is in-scope of your program. It's common for organizations to exclude some types of third parties from their program.

Your organization must decide which types of third parties or vendors you'll include in the TPRM program. For example, public utilities provide products and services to your organization, but your organization can't influence or control pricing, service, manage risks, or negotiate the contract. Moreover, public utilities provide their products and services to everyone, which means your organization isn't uniquely deciding to take on the risk associated with the public utilities' services.

Here are some examples of third-party types typically excluded from TPRM programs:

- Government entities
- Public utilities
- Sponsorships or donations
- Subscriptions for media, magazines, stock photography, social media sites, etc.
- Payees (including payments for a legal settlement or payments to board members or investors)
- Professional associations or conferences
- Products or services offered as an employee perk (the employee must engage directly with the vendor for these services)

Planning & Risk Assessment

Planning

Establishing a vendor relationship begins with clarifying why the vendor is needed and identifying the product or service's intended benefits. You also need to decide who will be responsible for the vendor engagement and whether they have the expertise and resources to do so. This individual will ensure that all necessary third-party risk management activities are completed on time and to the expected standard.

Identifying the Risk and Criticality of Each Vendor Engagement

Is your vendor critical? From the beginning, it's important to determine if your vendor engagement (product or service) will be critical to your operations

or customers. A vendor is critical when its failure, or sudden loss, would substantively impact your operations, making business as usual (or at all) impossible. Keep in mind that auditors and regulatory examiners often focus on critical vendors.

Three questions can be used to determine if your product or service (and vendor relationship) might be critical:

1. Would a sudden loss of this vendor cause significant disruption to your operations?
2. Would that disruption impact your customers?
3. If the time for the vendor to recover operations exceeded 24 hours, would there be a material negative impact on your organization?

If you answer “yes” to any of these three questions, you’re probably dealing with a critical vendor.

Inherent Risk Assessments

The vendor owner (or other identified individuals) must also complete an inherent risk assessment to determine which risks your vendor may pose to your organization or its customers. This typically involves completing a short questionnaire. Inherent risk questionnaires are internal documents and are always completed by the vendor owner.

PRO TIP

It's important to remember that no two vendors or vendor engagements are created equal.

This means you must assess every vendor AND every product/service you use, even if one vendor provides multiple services. A vendor-only assessment will greatly increase the likelihood of missing risks unique to the products and services.

Remember, an inherent risk is one that is naturally associated with a product or service and is assessed without examining any controls. Your inherent risk assessment should examine the types and amounts of risks in a vendor engagement. Not all types of risks are present in every engagement.

Let's examine the most common risks identified through an inherent risk assessment.

Types of Vendor Risk

Business Continuity and Disaster Recovery
This risk is present when the vendor has inadequate plans or hasn't tested their plans to maintain operations (at an acceptable level) during or after a business interrupting event.

Compliance
If the third party doesn't adhere to laws, regulations, guidelines, and industry specifications, then there's substantial compliance risk present. Compliance risk can also occur if a vendor fails to meet your organization's rules and requirements.

Cyber (Information Security)
Information security risks can be cyber or physical security-related risks. Cyberattacks and data breaches are the most common events that stem from missing or ineffective cyber controls.

Financial
The vendor may pose a financial risk if there's a decline in earnings or pending litigation, as these trends can impact their ability to service your organization.

Operational
This type of risk occurs when products/services, channels, or processes are critical to your organization's operations. Assessing operational risk can help determine if a vendor is critical.

Reputation
If a third party interacts directly with your customers and they provide poor service, have a data breach, or misuse customer data, it's your organization's reputation that will be harmed.

Strategic
There's risk present if the third party offers products/services that aren't compatible with your organization's goals, can't be effectively monitored by the organization, or doesn't provide an adequate return on investment (ROI).

Transactional
If the vendor handles any payments on your behalf, there's transaction risk.

Other
The risk categories aren't limited to the ones previously mentioned. Other risks, such as geopolitical, concentration, and environmental, social, and governance (ESG) risks, are categories that many organizations are now including on their inherent risk assessments.

A note about risk ratings: "Critical" should never be used as a risk rating, but rather as a label to identify those vendors that pose the most operational risk to your organization or its customers. For example, most critical vendors also have a risk rating of HIGH, but not every vendor with a high-risk rating is critical. It's important to make this distinction in your program. Additionally, almost all regulations dictating third-party risk management have specific requirements for critical vendors, so identifying them is essential.

When the inherent risk assessment has been completed, your organization should have two pieces of important information:

1. If the vendor is considered critical or not
2. The risk rating for the vendor engagement

These two data points are going to inform everything you do to manage the vendor moving forward, including the scope and depth of due diligence required, how the contract should be structured, the appropriate timeframe for re-assessing risk, what level of risk and performance monitoring is required, and considerations for offboarding the vendor if the time comes.

BEST PRACTICE

Effective third-party risk management demands a risk-based approach.

No program is going to have the time or resources to treat every vendor engagement with the same amount of rigor. So, ensure you're applying "the principle of proportionality," which means the higher the risk, the more robust the risk management must be. For example, a critical or high-risk vendor requires the highest degree of due diligence, frequent risk monitoring, and purposeful contract negotiation and structure. At the same time, a vendor with moderate risk may only require minimal due diligence and occasional monitoring.

Due Diligence

Due diligence is an essential and fundamental part of the third-party risk management lifecycle. Due diligence enables your organization to verify that the vendor is a legitimate business entity with a solid reputation and that the vendor has the appropriate controls to manage product and service risks.

A note about due diligence: Due diligence is not a one-time exercise. Effective third-party risk management requires periodically taking a fresh look at the vendor's controls and reputation. Your initial due diligence will set the stage for subsequent rounds of the verification process, where you will confirm existing controls are still sufficient and look for controls to address new and emerging risks.

The level of due diligence necessary is determined by the risk rating. No matter the risk rating, you must assess a vendor's legitimacy and reputation.

To confirm that your prospective vendor is a legal business entity, you can review the following:

- Basic information (i.e., full legal name, address, all physical locations, website URL)
- Any "doing business as" or "also previously known as" (d/b/a, aka, pka)
- Ownership structure and affiliated companies
- Tax ID
- State of Incorporation
- Articles of Incorporation
- Secretary of State Check
- OFAC/PEP Checks
- Business License
- Picture or Google map view of the facility (if required)

To assess your vendor's reputation, consider reviewing the following resources:

- Credit report
- Dun & Bradstreet (D&B) Report
- Vendor complaints research findings
- Vendor negative news search findings
- List of subcontractors/fourth parties
- Conduct a check of the CFPB Complaint Database and/or Better Business Bureau rating
- Vendor references

Validating a Vendor's Controls

The primary objective of the due diligence process is to validate that a vendor has the necessary controls to address identified risks. This process entails:

- **Vendor due diligence questionnaire**
  Completed by the vendor, these comprehensive questionnaires ask about specific risks and the vendor's practices and controls to manage them.

- **Vendor due diligence documentation and information**
  In support of the vendor due diligence questionnaire, a vendor must provide documented evidence of their controls.

- **Review and assess the vendor questionnaire and supporting evidence**
  A review of both the questionnaire and documented evidence must be completed by qualified and credentialed subject matter experts (SMEs). Typically, there is an individual SME responsible for each risk domain (cybersecurity, finance, compliance). SMEs are responsible for reviewing and assessing the vendor's business practices and controls and providing a qualified opinion regarding their sufficiency. SMEs should also provide an opinion about whether you should proceed with the engagement based on the sufficiency of the controls. Finally, an SME documents their findings in an official report.

Examples of Vendor Evidence Documents

During due diligence, vendors are required to provide documentation that proves their controls. By carefully reviewing these documents, the SME determines whether the existing controls are suitable for managing the risks, or if additional or different controls are required. In a due diligence review, several types of documentation may be used. The following are some examples of common due diligence documents:

- **System and organization controls (SOC) report**
  A SOC report is an independent audit report performed by a public accounting firm. The report will attest to the existence and effectiveness

of your vendor's controls. The report should tell you if your vendor has adequate controls in place to safeguard your data and if those safeguards are working based on the scope of the audit determined by the vendor. SOC reports are an important resource to help you understand the controls in place and determine whether the controls need to be improved.

- **Business continuity plan/disaster recovery plan (BCP/DR)**
  A business continuity plan ensures that the vendor's significant operations and products/services continue to be delivered in full or at a predetermined and accepted level of availability during and after a business interrupting event. The disaster recovery plan outlines the processes and procedures the vendor must perform to resume operations following an incident. These documents help you understand the vendor's action plan should an unexpected event occur that impacts their operations. It ensures that their preparedness meets or exceeds expectations and your own business continuity and disaster recovery plans.

- **Compliance policies and evidence of employee compliance training**
  Your vendors must provide evidence that they recognize and comply with all laws and regulations. A review of a vendor's internal compliance policy and proof of employee compliance training can provide insight into a vendor's compliance practices.

- **Cybersecurity plan**
  A cybersecurity plan identifies the vendor's cybersecurity posture by discovering any weaknesses and gives you the information to communicate any requests to strengthen the vendor's controls. The plan helps protect your organization from vulnerabilities that could cause a third-party data breach.

- **Financial statement**
  A financial statement identifies the financial health of your vendor. It helps protect your organization by providing a better understanding of

the vendor's financial posture and the ability to determine if the vendor can continue to provide a secure, safe, and quality product or service based on their financial viability. A year-over-year financial decline may indicate underlying concerns you'll want to address, such as pending litigation or service level issues.

Reviewing documented evidence of a vendor's controls is the minimum requirement. However, additional information may be considered as part of the due diligence process. This might include references from your vendor's customers, interviews with the vendor's senior management, and on-site visits.

PRO TIP

On-site visits aren't always necessary, and the requirements warranting one will vary across industries.

However, as a best practice, you should consider a site visit for any new critical or high-risk vendors. Benefits of an on-site visit include the opportunity to test the vendor's physical security controls. In addition, meeting the vendor's staff can strengthen your relationship and demonstrate to the vendor that your organization takes third-party risk management seriously.

At the completion of due diligence, your organization should be able to determine if it can safely proceed with the vendor engagement. In some cases, there may be findings discovered during due diligence that require remediation before moving forward. SMEs should review all remediation evidence before proceeding with contracts in such situations. If a longer-term remediation plan is acceptable, ensure you include the requirements and timeframe for remediation in your contract.

Contracting

Vendor contract management is the administration of written agreements with third parties that provide your organization with products or services. It includes negotiating the terms of contracts and ensuring compliance, change management, and ongoing maintenance of the relationship. It's the process of coordinating contract creation, execution, and analysis for the purpose of financial benefit, service delivery, and risk management for your organization. A well-written contract is your best proactive insurance against unexpected problems.

Here are four of our contract recommendations:

1. **Consider the entire relationship** and lifecycle while creating the contract.
2. **Determine what information and items you will need from the vendor** throughout the course of the relationship. Be sure to also think about your exit strategy should the relationship terminate (because it happens!).
3. **Be involved in the contract drafting process** to ensure that your specific requirements are included. You should request the inclusion of essential provisions such as breach notification requirements, a zero-trust model, and the required documents that you'll need to assess during due diligence.
4. **Be sure to centralize and standardize your contract process** so that you can easily repeat the process for future vendors.

PRO TIP

Your organization has the most leverage over a vendor before you sign the contract, so you should carefully consider the terms and provisions before executing any contract. Here are three reasons why:

1. Vendors are usually more flexible when negotiating terms, conditions, and pricing prior to initial contract execution.
2. All parties are bound to the terms agreed upon once the contract is signed, so you should take the old saying, "if it isn't in the contract, it won't happen," seriously.
3. Your organization is liable for any issues discovered after the contract has been executed. Before signing a contract, your organization is expected to conduct due diligence in accordance with regulatory and best practice requirements. Take time to review the contract carefully to make sure all necessary requirements and expectations are clearly documented.

At a minimum, your organization should make every effort to include these 14 major terms or conditions in contracts for critical and high-risk vendors:

1. Scope
2. Cost and compensation
3. Performance measures and standards
4. Reporting
5. Right to audit
6. Compliance
7. Ownership and license
8. Confidentiality and security
9. Indemnification, insurance, and liability
10. Dispute resolution
11. Default and termination
12. Customer complaints
13. Subcontracting and disclosure of critical fourth parties
14. Business continuity and disaster recovery plans and testing

Service Level Agreements

Consider adding specific service level agreements (SLAs) to the contract as it's being developed. An SLA outlines the non-negotiable standards or performance your organization expects from a vendor.

Your SLAs should state the following:

- Metrics
- Responsibilities
- Expectations
- Timing and frequency
- Any penalties or required remedies when SLAs are not met

PRO TIP

In vendor-written contracts, most SLAs favor the vendor since they contain standard service levels that they provide. Whatever the vendor contract states, don't accept these terms as non-negotiable. Instead, view them as a starting point for negotiations.

Once your contract is executed, your organization will need to stay informed of key dates related to that contract, including the timeframe for renewal. It's essential for your organization to perform a contract review at the halfway point of the contract term. For example, if you sign a contract that is effective for three years, then a contract review is appropriate at the 18-month mark.

Establishing this contract management practice allows your organization to consider any contract improvements or desired amendments well in advance of the contract renegotiation period. Remember, the less time you have to negotiate, the less leverage your organization has.

Ongoing

Once your contract has been executed and your vendor is in a business-as-usual state, the vendor relationship moves to the ongoing stage of the lifecycle.

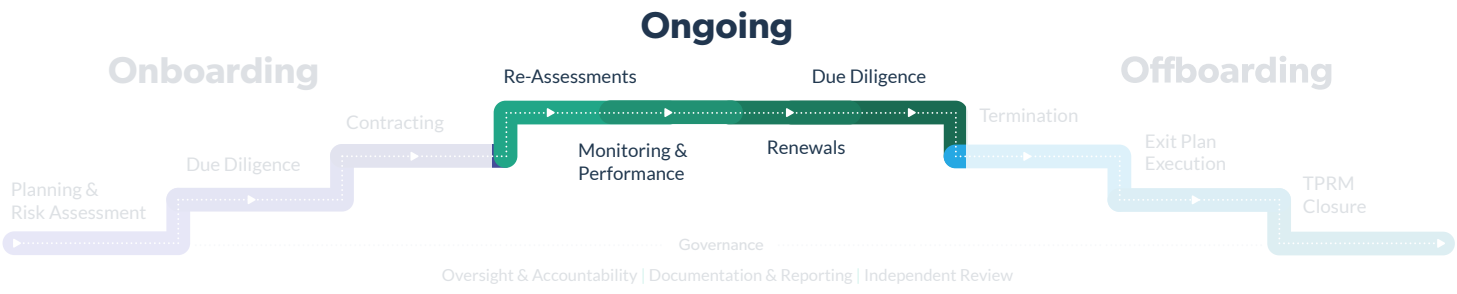
The ongoing stage of the third-party/vendor risk lifecycle involves constant and consistent risk and performance monitoring, periodic risk reassessment, and due diligence to identify and address any new or emerging risks.

Since risks can emerge, change, and evolve throughout your relationship with your vendor, it's necessary to keep your eye on the vendor relationship and identify potential trouble spots including:

- Faulty security controls
- Financial deterioration
- Poor performance
- Customer complaints
- Contract gaps
- Risky behavior
- Declining service levels

The activities required to assess, monitor, and manage the vendor repeat on a regular cadence during the ongoing stage, with required intervals for each activity based on the risk and criticality of the vendor relationship.

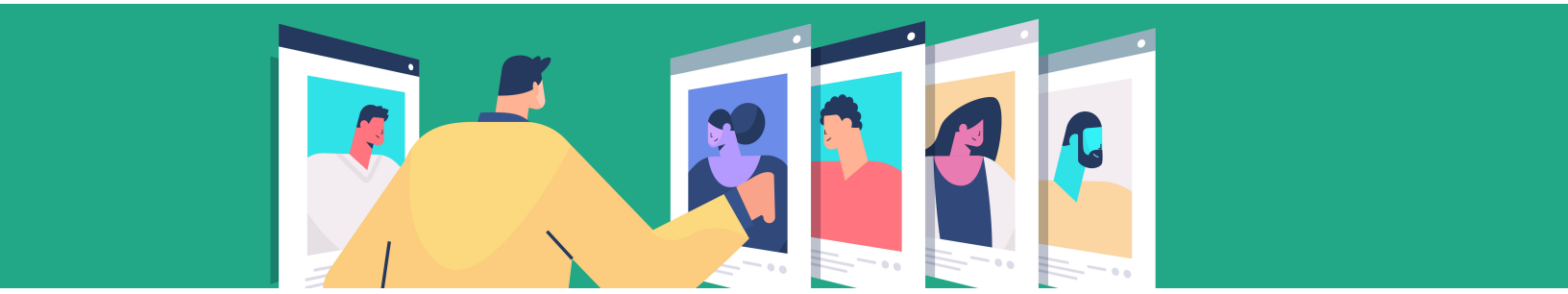
Let's explore the required activities for the ongoing stage.



Risk Re-Assessments and Due Diligence

A vendor's risk profile can change rapidly due to management or ownership changes, regulatory updates, financial pressures, industry shifts, cyber events, or any number of variables. A vendor who was great last year might turn out to be your worst vendor this year. Without a consistent process to identify the current vendor risk on a regular basis, your organization could find itself in a bad situation.

To avoid unpleasant surprises, your organization will need to review and update the inherent risk assessment on a regular and predictable basis. Once the inherent risk assessment has been updated, it's time to proceed with the due diligence review and update process. Keep in mind that if there have been changes to the vendor's inherent risks, you'll need to ask for updates to the vendor's due diligence questionnaire and new due diligence documents.



Due Diligence Review and Update

Even if there hasn't been a change in inherent risk, it's still important to ask the vendor to review and update their current due diligence questionnaire and documentation. At a minimum, the vendor will need to review the information your organization has on file and confirm that it's still accurate.

Vendor due diligence questionnaire

The vendor should be asked to review the current questionnaire to validate that the answers provided are still accurate and provide new information, if necessary.

Vendor due diligence documents

The vendor must confirm that existing documents are the most recent or provide updated documents. Examples of these documents include:

- **Independent third-party audits** such as a SOC report must still be effective, or the vendor must provide a bridge letter attesting that the controls are still in place. The vendor must also provide the date when the new report will be available.

- **Business continuity and disaster recovery plans** should be current and include the results of the most recent testing, including any issues discovered during testing and remediation. Critical and high-risk vendors should test their plans at least annually.

- **Internal policies** such as compliance, privacy, information security, etc., should be current. Regardless of whether a policy has been changed, a vendor should demonstrate an annual policy review.

- **Certificates of insurance** should be valid and current with the appropriate coverage types and amounts.

- **Financials** should include the most recent audited financial statements or the vendor's most current financial reports.

Remember that any vendor due diligence questionnaire or documentation changes will require a SME's review and report.

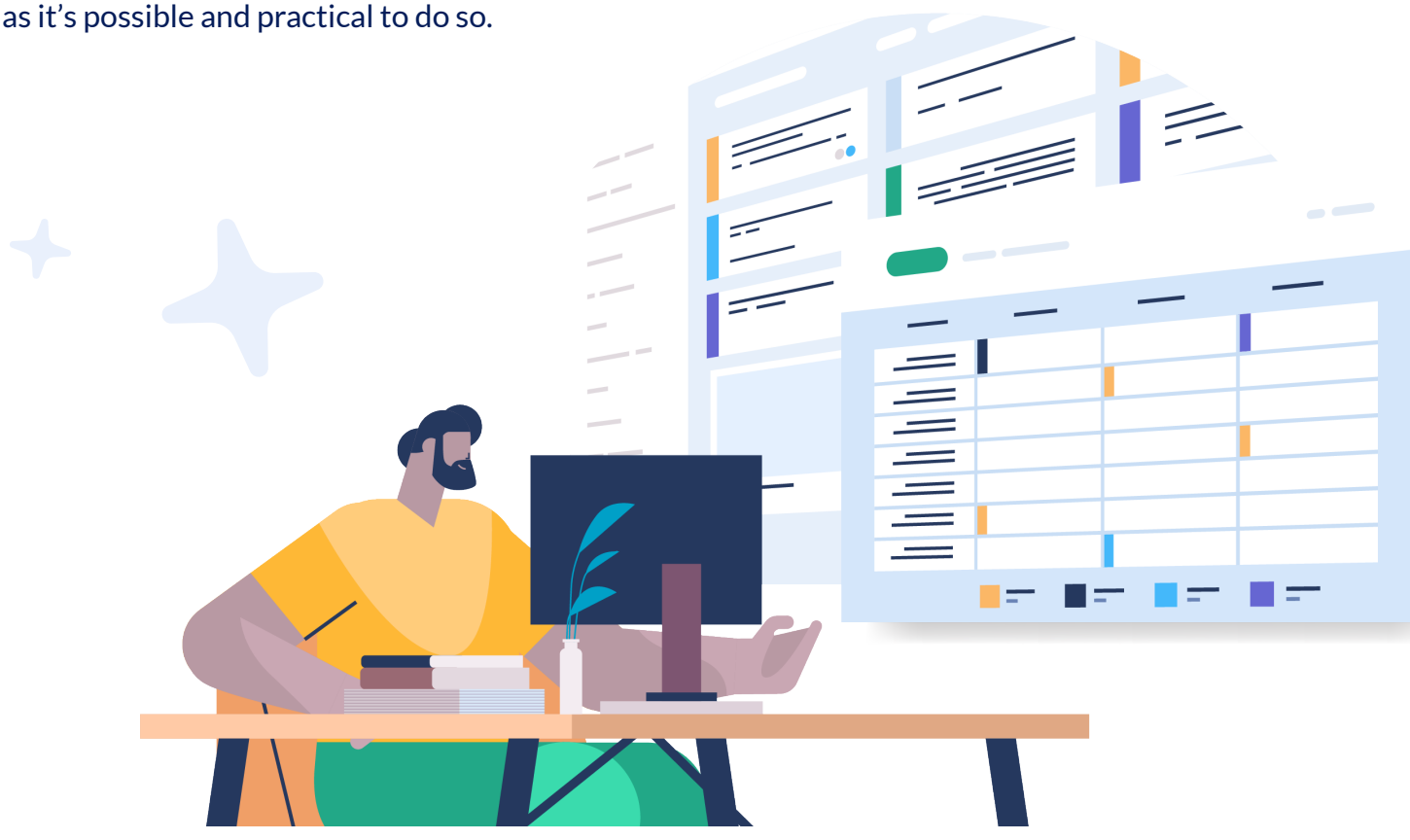
When to Periodically Re-Assess the Risk and Conduct Due Diligence

How often should you perform re-assessments? Well, that depends on the vendor relationship. As a best practice, as risk increases, the frequency of reviews increases.

Recommended intervals for this process are as follows:

- **Critical and high-risk vendors** should be assessed at least annually
- **Moderate-risk vendors** should be assessed every 18 months to two years
- **Low-risk vendors** should be assessed prior to contract renewal or every three years

If there are any known risk or performance issues, industry or regulatory changes, or changes in the vendor's management or ownership, your organization is encouraged to re-assess risk and update due diligence as soon as it's possible and practical to do so.



Monitoring & Performance

Ongoing risk and performance monitoring are essential to determine whether your vendor has lived up to its contractual requirements and expectations and to identify any new or emerging risks that could impact your organization or customers.

Performance Monitoring

Performance monitoring is the activity used to evaluate if the vendor is meeting your expectations and confirm that your organization is getting the intended benefits from the relationship.

Performance monitoring is also an ongoing activity, which means that it happens all the time on a day-to-day basis. By regularly monitoring (and managing) your vendor's performance, you can easily identify and remediate small issues before they become big problems.

When looking at the vendor's performance, you should ask yourself the following questions:

- Is the vendor meeting the expectations and standards laid out in your contract and SLAs?
- Is vendor performance stable, improving, or declining?
- What are the risks of poor performance?
- Are the vendor's products and/or services worth the cost and risks?
- Has the cost/risk-to-benefit ratio changed enough for you to consider ending the relationship?

You should formalize your performance monitoring by holding a regular performance review with your vendor. Depending on the products or services provided by the vendor, your performance review schedule may vary. The recommended cadence is:

- **Critical and high-risk vendors:** At least quarterly (but can be more frequent depending on the product or service type)
- **Moderate-risk vendors:** At least every six months
- **Low-risk vendors:** Annually or prior to contract renewal

If your vendor hasn't met your agreed-upon standards and requirements, or if the cost and risks exceed the benefit of the vendor's services, it may be time to consider exiting the relationship.

Performance Monitoring

Just like performance monitoring, your organization will need to monitor its vendor's risk constantly. Unsurprisingly, declining vendor performance is often a sign that there are hidden or emerging risks. Other factors, such as a change in management or ownership, losing a major customer, lawsuits, or excessive consumer complaints can dramatically alter a vendor's risk profile.

Still, it's important to remember that vendor risk isn't always just about the vendor and their internal practices. Regulatory changes, industry shifts, consumer behaviors, business interrupting events (such as the COVID-19 pandemic), or geopolitical conditions can all affect vendor risk. Some of these external risk influencers can be hard to predict and aren't always easy to spot. For this reason, many organizations are turning to outside resources to supplement their risk monitoring practices. Some of these resources include:

- Setting up internet news alerts for the specific vendor, industry, and regulator
- Subscribing to risk alert and monitoring services that provide target risk intelligence at the vendor and industry levels
- Participation in industry forums or peer groups
- Regular review of regulatory websites and social media

PRO TIP

Between your formal risk and performance reviews, it's important to communicate with your vendor on an ongoing basis about any potential gaps, concerns, and performance requirements. Keeping an open dialogue is the best way to ensure that new or emerging risks or issues are identified and managed effectively.

Contract Renewals

As part of the renewal process, you should review your contract at the midpoint of the contract term to identify any necessary changes or terms you would like to renegotiate to make the contract as effective as possible. Don't wait until the contract is up for renewal to conduct this analysis. This practice will help your organization maintain a continuous and efficient process that will prevent rushing through contract negotiations.

Your organization may decide against contract renewal for various reasons, including:

- Risk or performance issues
- Pricing
- Desired changes to the product or service
- Technology considerations
- Discontinuation of the product or service
- Conclusion of the project

Regardless of why your organization is choosing to terminate the contract, it's essential to follow the termination conditions of the contract and provide your vendor termination notice within the acceptable time frame. Failure to adhere to these contract conditions can result in early termination fees, litigation, or reputational damage.

Offboarding

For one reason or another, vendor relationships end. In these times, it's important to understand the best practices for offboarding your vendor and creating an effective exit strategy to follow when a contract ends.

Termination

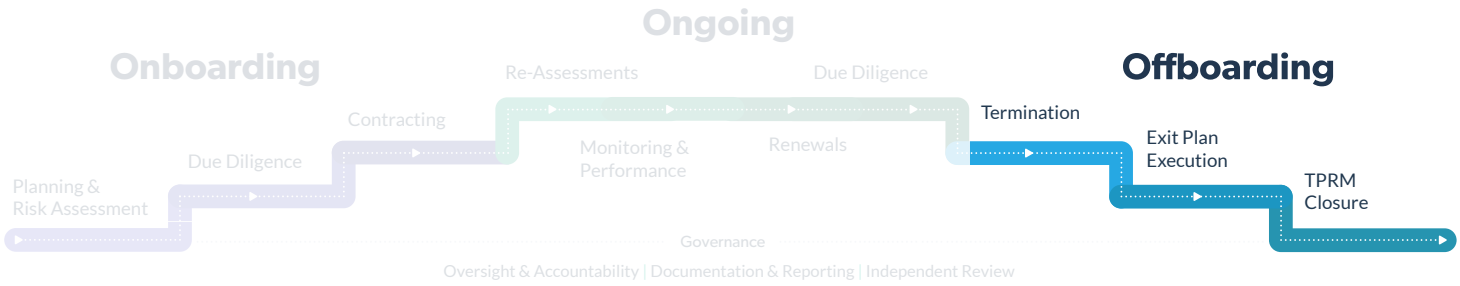
When you've determined that you won't be renewing a vendor contract after it expires, you should notify your vendor of your decision. Remember that the vendor engagement isn't officially terminated until the date that's stated on your contract.

Exit Plan Execution

Your organization should have a detailed plan in place that covers the various tasks and responsibilities that your organization and vendor will need to carry out when the contract expires. Be sure to thoroughly follow this plan. Necessary activities and plans may include instructions for your vendor to return or destroy sensitive information, or for your organization to remove the vendor's access to privileged networks and facilities.

TPRM Closure

During this step of the offboarding stage, you should handle the final tasks of closing the vendor relationship following your exit plan. You should tie up any loose ends at this time, such as reviewing and paying any final invoices and filing all relevant vendor information in an archive that can be accessed later, if needed.



Best Practices For the Offboarding Stage

- **Communicate your decision to leave the relationship with your vendor.** While the relationship won't officially end until the contract's expiration, you should let your vendor know your intentions.
- **Develop an exit plan with clear roles and responsibilities for you and your vendor to follow.** This should include returning sensitive materials, limiting access to privileged accounts and data, and deciding how you will fill the gaps (i.e., will you be bringing on another vendor or handling the services in house?).
- **Follow through with any final steps after the relationship's close.** For example, this could include reviewing and completing a final invoice or stopping payments from occurring in the future.
- **Closeout and appropriately archive vendor records from all systems.** Make sure these records are organized and accessible in the event of an audit or exam.

Foundation of the Third-Party (Vendor) Risk Management Lifecycle

Now that we've covered the activities in the third-party/vendor risk management lifecycle, it's time to consider the foundation of the lifecycle and examine the various elements that support your program.

Oversight & Accountability

It's not enough to have a great process. It takes oversight and accountability to ensure an optimal TPRM/VRM program. Review your program to ensure the following:

- The board and most senior management are informed and engaged, hold people accountable, and set the tone-from-the-top.
- The board or most senior management is responsible for reviewing and approving your third-party/vendor risk management policy.
- All stakeholders have clear roles and responsibilities.
- Stakeholders are held accountable when they fail to uphold their responsibilities.
- There is a defined issues escalation process.

Documentation & Reporting

Governance documentation is a vital component in every TPRM/VRM program. Your governance documents must clearly identify the rules, tools, processes, and procedures integral to your program and often include:

- Third-party or vendor risk management policy which includes the formal rules and requirements of the program.
- Program document which describes the processes necessary to meet the rules and requirements of the policy.

- Procedures that detail the steps and actions required to execute the processes.

Vendor documentation must be appropriately preserved, organized, and associated with the vendor's record, including all vendor due diligence questionnaires, documents, SME reports, performance reviews, and copies of vendor communications. These documents must also be easily accessible in the event of an audit or exam.

Other documents, such as internal TPRM training decks, communications, and presentations, should be preserved as evidence for audits and exams.

Reporting is a key element of any TPRM/VRM program. Program reporting should include board-level reports, risk committee reports, issue management and escalation, compliance, and other stakeholder-specific reporting.

Independent Review

To ensure your TPRM/VRM program is operating effectively, there must be thorough periodic reviews conducted by unbiased independent reviewers. These reviews may come in the form of internal or external audits or even regulatory examinations. External standard-setting and certification organizations may also provide independent reviews.

Effective third-party/vendor risk management consists of a broad collection of interdependent processes, activities, rules, requirements, and stakeholders that requires an organized approach.

Using the third-party/vendor risk management lifecycle as your roadmap, you can ensure that vendor risk is comprehensively identified, assessed, managed, and monitored throughout the vendor relationship.

Download free samples of vendor Control Assessments and see how Venminder can help reduce your third-party risk management workload.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.