A GUIDE TO

The Third-Party Risk Management Lifecycle

venminder

Guide to the Third-Party Risk Management Lifecycle

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.

Regardless of your industry, it's recommended that you understand the best practices so you can optimize your vendor management program and resources. This eBook offers a practical, risk-based framework to identify and mitigate inherent risk while also explaining ongoing and offboarding activities. Our goal is to guide you throughout the entire third-party risk management lifecycle which in turn will help you understand how to protect your organization and its customers from vendor risk.

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

Regulatory compliance can be achieved by following the practices outlined in the third-party risk management lifecycle.

Third-Party Risk Management Lifecycle

Guiding the Lifecycle

Before jumping into the third-party risk management components, you must first understand the foundational elements of oversight & accountability, documentation & reporting and independent program review. These essential components support and guide the lifecycle.

Oversight & Accountability

Every organization should define and document where third-party risk management resides internally, who is responsible, and subsequently, how the various steps and functions are managed. It's necessary to identify who is responsible and accountable for accomplishing each task and function.

Often, third-party risk management requires support from various departments, such as information security, business continuity and/or disaster recovery, enterprise risk, compliance, legal and/or sourcing. Not only should responsibility and accountability be clearly defined, but stakeholders across the organization must be educated on the process. Decision makers should be aware of how the third-party risk management program exists within the broader framework of your organization.

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

Important Questions to Ask

1. Who is responsible for managing vendor contracts?
2. Who is responsible for managing the overall vendor inventory?
3. Who conducts the risk assessments and collects due diligence?
4. Who is accountable for managing the risks identified as part of vendor engagements?
5. Where and to whom are vendor risks reported?
6. Who will monitor and escalate issues as required?

Documentation & Reporting

The following are standard governance documents and reporting examples used to define third-party risk management objectives, roles and responsibilities and the expected outputs of the processes defined therein.

Policy:

What must be accomplished? A policy document is generally a concise depiction of intent of what needs to be accomplished as an organization. Deviations from a policy should only occur by way of a formal exception. A good rule of thumb would be to keep it simple while still observing regulatory responsibilities.

A third-party risk management policy would generally cover, but is not limited to, the following areas:

- Policy, Statement and Purpose
- Scope and Organization
- Roles and Responsibilities
- Risk Tolerance, Accountability and Metrics Requirements
- Risk Assessment and Vetting Processes
- Conducting Due Diligence
- Contractual Standards and Management
- Oversight and Ongoing Monitoring
- Termination and Exit

Program:

How should the policy be implemented? A program document is often an excellent way to supplement policy documents by going into more detail on the structure for how your organization should meet policy requirements. A program document may include a drill down of responsibilities, how departments should work together, itemize the deliverables and functions needed for the process to run smoothly and mention specific reports. Metrics can also be defined in more detail if not already included in the policy.

Procedures:

What are the steps to accomplish requirements? Ideal procedures are documents that anyone could pick up, follow the steps and produce the necessary work products. Procedures are essentially the secret sauce of day-to-day tasks and activities.

Additional Supplemental Documents:

Sometimes, additional documents are needed as they're part of the overall process and required by the governance documents. These additional documents may include information gathering questionnaires, risk assessment summaries, exception requests and reports. These document types represent controls that tie to audit requirements and demonstrate that specific process steps are fulfilled, so they're often defined as requirements in the governance documents.

Reporting:

Reporting requirements should be defined in policy and program materials regularly provided to appropriate stakeholders and may include:

- Analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the banking organization.
- A current inventory of all third-party relationships, which identifies those relationships that involve critical activities.
- Reports for critical relationships detailing the current status of risk assessments, due diligence results, contract status, performance, service levels, internal control testing and other ongoing monitoring results.
- Third-party service disruption, security breaches or other events that pose a significant risk to the organization.
- Third-party risk management program metrics, issues, tests or other relevant information.

PRO TIP

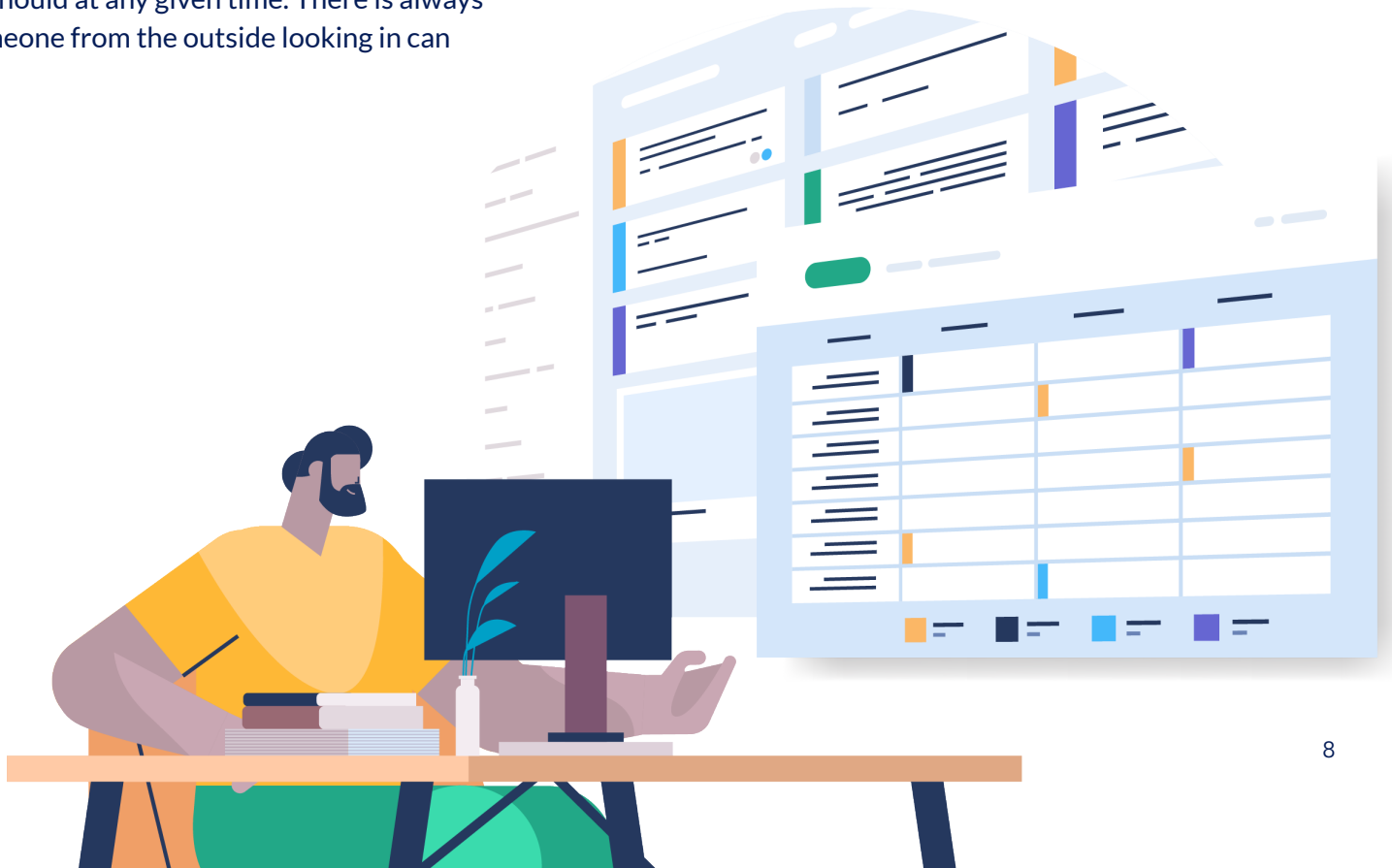
It's important to keep both formal and informal documentation.

A vendor database should be seen as the appropriate place to store and maintain vendor data, documentation, risk metrics, issue and risk management notes and any other relevant documentation.

Independent Review

All of your third-party risk management notes, key documents, metrics and reports are an essential part of supporting and providing evidence for your independent review. It's one thing to have stellar governing documents in place, but they don't mean much when you can't prove that you're compliant with them.

Consider outside reviewers, like independent audit and third-party assessors, as assets – ones that can keep you honest and help ensure your program meets regulatory guidance. Outside reviewers should put you to the test to make sure you can prove that you're doing what you should at any given time. There is always room for improvement and sometimes someone from the outside looking in can provide extremely valuable feedback.



3 STAGES OF

Third-Party Risk Management Lifecycle

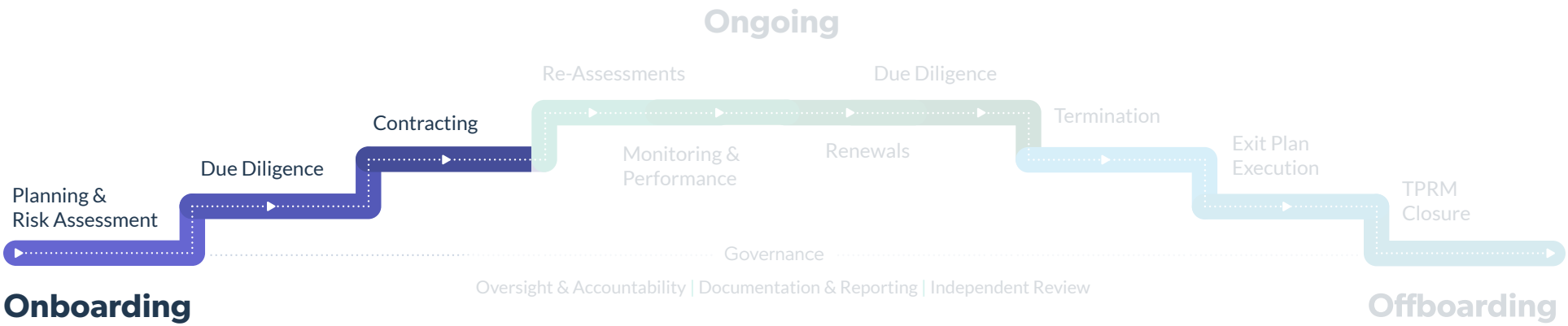
Now that we've covered the foundational supporting elements of the third-party risk management lifecycle, let's move on to the recommended path in a robust third-party risk management process.

STAGE 1:

Onboarding

Bringing a new vendor into your organization requires careful planning and consideration to ensure that the engagement is built strong from the start. It's essential to fully understand the amount and types of risk that your organization will need to manage way before you get to the point of selecting a vendor and signing the contract.

The following activities are involved in the onboarding process:

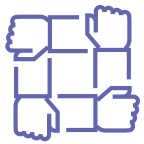


1 Planning & Risk Assessment:

Before you begin the onboarding process, it's necessary to establish a clearly defined scope for what needs to go through the third-party risk management lifecycle. Customers, clients and business partners will generally be excluded from this process. Create a repeatable process to define what a vendor, service provider or third party is to your organization.

Once you know that the third party is in scope for your third-party risk management process, you'll need to identify the inherent risk of the engagement and whether the product or service (and vendor) is considered critical to your organization's operations.

Inherent risk naturally exists as part of the product or service (and the relationship by default). This is assessed without considering any existing or future precautions or controls. Inherent risk is often rated by a tiered system 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. Products and services necessary to sustain your core operations, interface with your customers or support your organization's ability to comply with regulatory requirements are all examples of critical vendor engagements. Every vendor should be rated as either critical or non-critical.

Determining the inherent risk and criticality is a crucial first step of any vendor engagement. Best practices dictate that an inherent risk assessment is conducted before signing an agreement. Knowing the risk and criticality of any vendor paves the way for appropriate and risk-based due diligence. And, it determines the frequency and intensity of ongoing monitoring activities throughout the life of the vendor relationship.

Remember, assessing risk is a continuous process that requires periodically validating that the relationship is still the same. Inherent risk assessments should be done for each product or service engagement, not just every vendor. Inherent risk and criticality generally won't change throughout the relationship.

EXAMPLE

Someone in your organization wants to sign on a new service from a vendor with whom you're already doing business.

Don't let that dissuade you from conducting a risk assessment on the new engagement.

Even if you've already conducted one for that vendor in the last year, the new engagement has its own inherent risk.

2 Due Diligence

Now that we understand the inherent risk and how critical that product or service might be, we can determine the best way to mitigate risk appropriately and effectively. Due diligence is the step that helps you determine if the necessary controls are in place to manage the identified risks appropriately. Put another way, due diligence is ensuring you've done your homework so you can be confident that you know the risks and have done the necessary work before drawing lines between your organization and another.

The due diligence process is generally achieved by collecting and validating information from and about the vendor and then taking into account controls that mitigate or reduce the inherent risk.

Here is a list of items, although not fully inclusive, which may help in providing the assurance needed by collecting and/or reviewing as part of the due diligence process:

Considerations for all vendors:
Basic information (e.g., legal name, doing business as, professionally known as, address, locations, website, ownership structure, etc.)
Articles of Incorporation or business license
Tax ID #
Liability insurance coverage/certificate of insurance

Additional considerations for vendors who are critical or have high inherent risk:
Completion of a questionnaire for any additional information needed to understand risk exposure and mitigation
Audited financial statements or the most recent financials, SOC 1, SOC 2 and SOC 3 audits, or any other information technology-related audit
Business resumption, contingency plans and testing summaries
List of all subcontractors or other parties that may have access to data or information provided by your organization or which are essential in providing services (i.e., your vendors' critical vendors)

When you have completed your review and evaluated the controls, you can now look at the residual risk, or the risk left over after applying controls. Based on your review, you may find that all the necessary controls are in place, the risk is mitigated and nothing further is needed.

Or, you may have concerns based on the due diligence results because the controls are inadequate or insufficient to reduce the inherent risk. In this case, further steps will be necessary for remediation. It starts by communicating the elevated residual risk to the right people.

Next Steps When Residual Risk Requires Attention

It's essential that all stakeholders, especially vendor owners, understand the residual risk and recognize and act on any open items that must be addressed and monitored.

Remediation efforts and risk metrics should always be well documented. Suppose mitigation is inadequate and the vendor isn't meeting their end of the bargain. In that case, the issue should be escalated to senior leadership to either accept the risk or determine any further actions.

Suppose serious issues are discovered during initial due diligence (meaning pre-contract during vendor vetting). If so, the best course of action is to consider a different vendor. However, on occasion, the residual risk for existing vendors may exceed your organization's risk tolerance. In these situations, there may be a need for formal corrective action plans, litigation or contract termination depending on the level of risk, criticality and contract terms.

Conducting due diligence helps you validate the following:

- The legitimacy and good standing of the vendor
- The effectiveness of mitigating controls
- The residual risk

3 Contracting

Vendor contract management is the administration of written agreements with third parties that provide your organization with products or services. Once you've established the inherent and residual risk levels and found them to be acceptable, it's time to consider the contract.

For new engagements, you can go ahead and write your requirements into the new agreement. You can use existing vendors' risk assessment and due diligence data to determine if any provisions should be made in the following contract review.

Contract management entails:
Having a process in place for internal planning, negotiating, creating/drafting, approving/executing, storing and managing contracts
Incorporating essential controls
Creating service level agreements (SLAs)
Managing key contractual dates

Contract Management Importance

Having a good handle on your contracts will save money and time. And, it may help you avoid unnecessary headaches like missing significant contract term dates! Contract management also establishes expectations to ensure your organization is protected from all areas of vendor risk.

New Vendor Contract Management

When negotiating new contracts, you can begin with either your standard contract template or the vendor's template. Be sure to build upon that template language and change terms and provisions as needed.

Aside from your standard contract terms, here are 5 important things to consider:

1. **Regulatory Compliance**
   Vendors might not be held to the same standards and regulations as you are, but they must be when they are working on your behalf. So, make sure to hold them accountable to YOUR standards in the contract as broadly as you can.

2. **Notifications**
   Ensure the vendor is required to notify you and work with you if they change anything that affects your organization. For example, you should be notified if the vendor switches data centers that hold your data.

3. **Software Service Levels**
   Be sure to include uptime and downtime requirements for software services. Consider penalties if a vendor exceeds their maximum downtime. This is especially important if the lapse in service would negatively impact your organization (i.e., critical applications).

4. **Termination**
   Having fair provisions for termination can go a long way in minimizing any future disruptions. Ideally, exit strategy provisions should be laid out in the contract and documented for any vendor with your data or performing critical processes. Try to make sure the strategy covers both a planned exit (gradual, intentional unwind) or an unplanned exit (sudden loss of a vendor). Have a plan to replace the vendor or bring the function back in-house.

5. **Right to Audit**
   Have vendors agree, in writing, to your organization's right to audit. Ensure you are allowed access to their policies, procedures and facilities at least once a year. Include the right to view (on request) third-party audit reports such as SOC documents and other information relevant to your business.

A well-written contract is the best insurance against unexpected problems.

In addition, check that these items are established:

Roles and responsibilities

Ensure roles and responsibilities are clearly identified.

The approval process

There should be an appropriate approval process for signing contracts such as senior management level approval for critical vendors.

Pre-contract due diligence

Completing due diligence before contract execution is required. No contracts should be executed until due diligence is complete and residual risk is considered acceptable.

A contract repository

A central and well-organized contract repository is necessary to track and manage contracts effectively.

PRO TIP

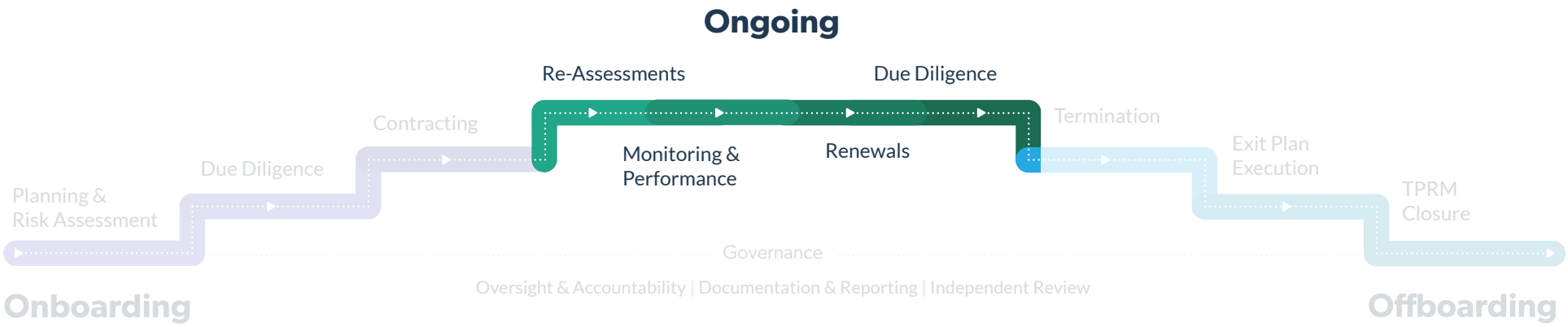
Vendor managers should have a close working relationship with the contract managers.

As the relationship continues, any issues discovered in periodic risk assessments should always be considered as contracts come up for renegotiation and vice versa.

STAGE 2:

Ongoing

Now that the planning & risk assessment, due diligence and contract execution are complete, the ongoing stage begins. After you sign the contract, ongoing monitoring of the vendor's risk and performance is extremely important. This step allows you to remain aware of any new or emerging risks or performance issues. Activities in this stage include re-assessments, monitoring & performance, contract renewals and due diligence.



Here's a deeper explanation of each activity:

1 Re-Assessments

For re-assessments, start by having your line of business or business owners confirm that nothing has changed with the relationship. This can be done by reviewing, and updating if necessary, the inherent risk assessment.

Once you've validated the inherent risk is the same, reach back out to the vendor to collect updated documents, assess the due diligence and update your residual risk accordingly. 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.

2 Monitoring & Performance

Ongoing monitoring of vendor risk and performance helps ensure that risk level and quality remain consistent throughout the relationship. This includes service level agreement (SLA) tracking and staying well-informed of any issues or changes.

Monitoring should include the measure of performance of third parties in terms of profitability, benefit and service delivery. The key questions become:

1. Are they living up to contractual obligations? (i.e., SLAs)
2. Is the benefit of the vendor product or service worth the measured risks and cost?
3. Has the cost/risk-to-benefit ratio changed enough to consider an exit?

You want to position yourself to be prepared if things start to go astray, if SLAs aren't being met or there has been a severe issue such as a data breach. It's important to keep a close eye on your vendor. Suppose there are changes in the vendor's internal processes or control environment for some reason. In that case, you'll need to understand how it might affect your organization and plan accordingly.

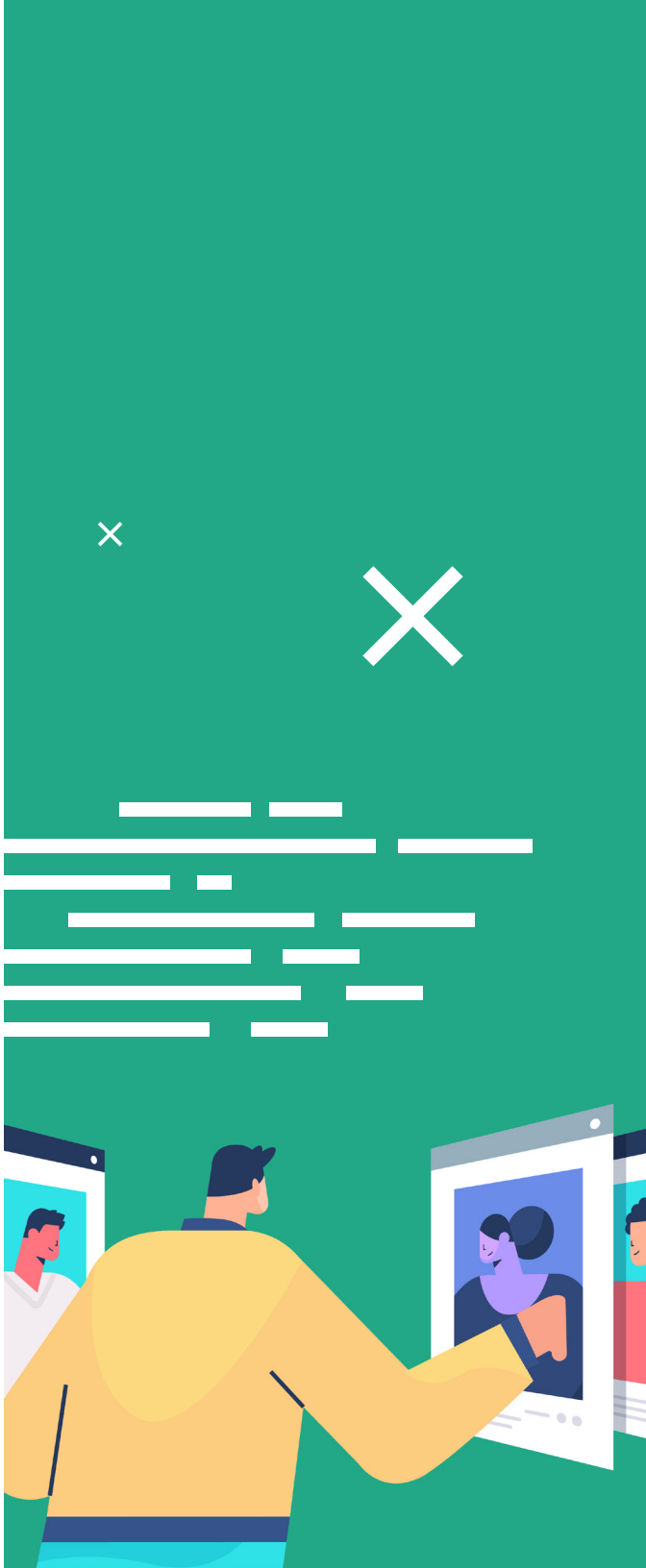
3 Renewals

Plan your contract renewals well in advance so you have sufficient time to negotiate any changes that may be needed. Negotiations can be time-consuming, so it's best not to wait to review the contract until just before the renewal period. This puts you at risk for a rushed process and decreased negotiating power.

As part of ongoing contract management, you should be having a continuous and consistent dialogue with your vendor. Discussions should include service delivery, performance, meeting specific requirements and addressing any service level gaps. Don't forget to track SLAs, enabling both parties to be accountable. As a best practice, most regulators and auditors are looking to verify that your contract management process is well developed, organized and maintained on an ongoing basis.

4 Due Diligence

Due diligence isn't meant to be a one-time activity done only at the beginning of a vendor relationship. A vendor's risk as well as their underlying controls can evolve over time, so regularly collecting and reviewing due diligence is important. Periodic due diligence reviews should be scheduled at least annually. They can also be done before contract renewals, if there are performance issues or if there are new or updated regulatory requirements.



6 Best Practices for the Ongoing Stage

To support a healthy routine of ongoing monitoring, it's necessary to do the following:

1. **Regularly run reports**
   Regularly report vendor activity to senior management and the board to keep them in the loop. Escalate as needed, too.

2. **Set up SLA tracking**
   SLA tracking is critical to understanding how a vendor performs, so be sure to set up tracking in your platform (or another method) to track these metrics.

3. **Use monitoring alert tools and services**
   If possible, subscribe to vendor risk monitoring and alert services. These tools support real-time alert notifications if something goes wrong with your vendor. They also help you monitor risk between formal risk reviews.

4. **Base your review schedule on the inherent risk rating**
   Always use your inherent risk rating as the basis for all vendor risk management activities. Even though your vendor may have a lower residual risk score, all risk and performance monitoring activities should be driven by the inherent risk rating.

5. **Set an ongoing monitoring standard**
   Your ongoing monitoring standards should make sense for your organization and consider your resources. However, as a general rule, critical and high-risk vendors should be reviewed at least annually, moderate-risk vendors every 18 months to two years and low-risk vendors every two or three years.

6. **Stick to your internal third-party risk management policy**
   Examiners will want to see that your work product matches what is stated in the policy.

The ongoing stage in the lifecycle is precisely that… ongoing. This is the stage of the third-party risk management lifecycle where most of your vendors will be at any given time. Remember that ongoing monitoring is a "team sport" that requires communication and collaboration between the vendor owner, third-party risk management, contract managers and other relevant stakeholders at the organization.

Here's an overview of how each of these roles usually contributes to managing third-party risk:

Third-Party Risk Managers

They're responsible for the third-party risk management framework, determining monitoring schedules and facilitating ongoing monitoring activities such as annual risk reviews.

Vendor or Product Owners

The individuals who utilize the vendor's services and own the engagement risk. Their ongoing monitoring tasks include tracking SLAs and liaising with the vendor appropriately if any risk or contract issues arise.

Contract Managers

Generally maintain contracts by keeping track of important dates such as when the contract is up for review and renewal. Suppose any contract issues arise, such as not meeting contractual requirements or concerns that may warrant negotiation for an amendment. In that case, contract managers should be in the loop.

PRO TIP

For re-assessments, start by having your line of business or business owners confirm that nothing has changed with the relationship.

Then, once you've validated your inherent risk is the same, reach back out to the vendor to collect updated documents, assess the due diligence and update your residual risk accordingly

These functions may vary or might be shared depending on how an organization is structured and how roles are delegated. Still, it's essential to understand and execute these activities individually.

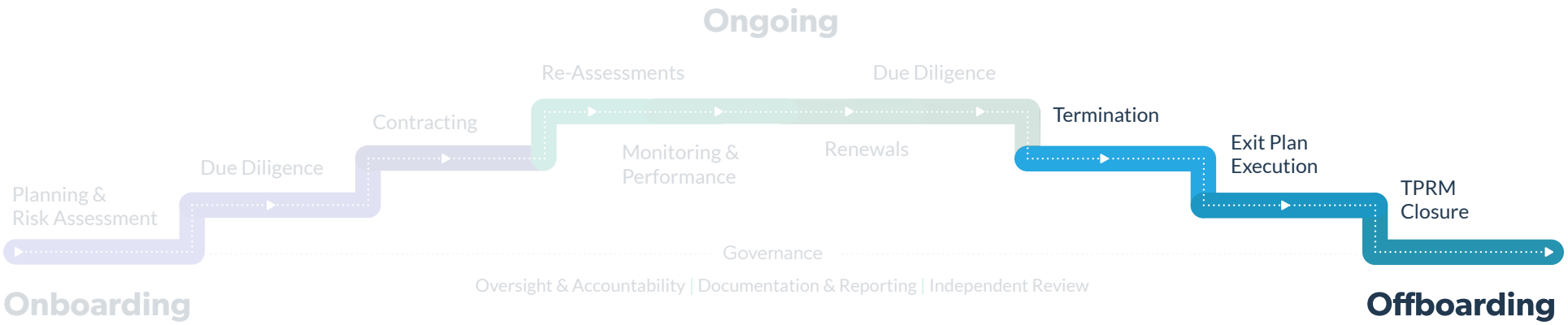
As long as you're leveraging a vendor for an outsourced product or service, you must maintain some level of ongoing monitoring.

STAGE 3

Offboarding

Finally, there comes a time when an engagement must come to an end, either proactively or reactively. For example, maybe because a vendor is shuttering, has failed to perform, the contracted term ended or you just need to move on to bigger and better things. There should always be some consideration into how the termination processes may look for any particular vendor.

In some cases, once the contract term has ended, there isn't much to do besides closing the vendor out of your system and removing them from the vendor inventory. However, you'll need to follow your exit strategy for more significant or critical vendors and make sure you're terminating the relationship per the contracted terms.



Here are the activities involved in the offboarding process:

1 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.

2 Exit Plan Execution

Your exit plan should clearly define the duties and responsibilities of both parties when the contract ends. The vendor must follow the proper return or destruction of sensitive data plan. 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.

3 TPRM Closure

Once the vendor exit plan is complete, you may still have a few final steps to close down the relationship formally. 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).

5 Best Practices to Consider
During the Entire Third-Party Risk Management Lifecycle

1. **There should be board and/or senior management involvement.**
Some leading regulators require the board to actively engage in the third-party risk management program. They're often required to have an awareness of the process especially when it comes to critical and high-risk vendors. Regardless of your industry or what regulators you fall under, board or senior management engagement is always a best practice.

2. **Report on your vendors.**
Third-party risk management is only as good as the data driving the practice. The information must get to the right stakeholders to ensure third-party risk management data is incorporated into your organization's business considerations and decisions. Effective and timely reporting enables better business decisions and risk management.

3. **Ensure risk assessments are timely.**
A risk assessment is completed during initial due diligence and as part of ongoing monitoring. Make sure you have a documented schedule compliant with your policy and aligns with your overall governance documentation.

4. **Document everything.**
If it isn't documented, then it essentially didn't happen. Regardless of the outcome, it's always better to document any elevated risk situation than to come up short during an audit or examination.

5. **Trust the process.**
The lifecycle is a tried-and-true way to meet expectations and defend against third-party risk. To use it effectively, remember that it's a continuous and fluid machine that you need to keep well-greased.

The lifecycle can help your organization stay on track and avoid vendor risks when applied effectively. Using the third-party risk management lifecycle to guide and inform your processes can make you feel confident that you're meeting best practices and protecting your organization from avoidable risks.

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

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.