FLIGHT PATH TO

Master Third-Party Risk Management

venminder

Table of Contents

Flight Path to Master Third-Party Risk Management

A lot of thought, processes, resources and individuals go into the makeup of a successful third-party risk management program. Sometimes, it's challenging to see the big picture and how you'll get from one destination to the next. In this eBook, we're going to share with you an extensive overview of third-party risk management covering many of the ins and outs that you should know.

Determine Your Third-Party Risk Management Model

To begin, let's start with third-party risk management models that can be used. Just like there are different designs of planes, there are different designs of a third-party risk management program. There are various ways that a third-party risk management function can be implemented within an organization. We typically see these three models:

- **Decentralized**
- **Centralized**
- **Hybrid**

Here is a little more about each:

Decentralized

A decentralized model is when there essentially isn't a formal third-party risk management program or team. The functions required for third-party risk, like risk assessments, due diligence and contract management, are shared among different areas, who may or may not share in some sort of collaborative reporting to leadership.

Challenges

In a decentralized model, it's really hard for one person to take care of all aspects of a vendor review, especially when it's not their primary responsibility. Sure, with more individuals involved, it lightens the workload, but this is still the least standardized, organized or effective model.

In a fully decentralized model, there tends to be little or no single authority to make sure things happen. Even if you set great standards, there will always be varying degrees of consistency which can lead to real issues, not only in protecting your organization from risks, but also in answering to audits and regulators.

PRO TIP
If you do opt to use a decentralized model, it's essential that there are people or persons responsible for verifying standards are being adhered to, or you could quite simply be setting yourself up for disaster.

Centralized

A centralized vendor management model would mean that there is a single, dedicated team, person or unit that manages all aspects of third-party risk management. It provides for much more oversight and accountability of all the tasks associated with vendor management, and this assists with more streamlined communication between the risk group and various areas of the organization.

It's important to understand that a centralized third-party risk management model must include experts of various disciplines, since cyber risk, fraud, business continuity, disaster recovery, financial health and potential litigation issues are a regular part of the process. As vendor management becomes increasingly more specialized, it's a requirement to have subject matter experts who can manage these various disciplines.

Challenges

Even though communication is often improved with a centralized model, it can also lead to certain stakeholders being out of the loop. For example, business units may not fully appreciate the risk of doing business with a particular third party. This can be a concern when they're primarily responsible for the daily interaction with the third party. And, in the fully decentralized model, there's a real danger of creating a disconnect between what you require in third-party risk management versus what the relationship manager may be discussing with the vendor each day. Items that are a high priority to you may get drowned out by the business needs or vice versa.

> **PRO TIP**
> *When using a centralized model, remain highly focused on communication and timely reporting.*

Hybrid

The hybrid approach is most often recommended, especially for a larger organization. This approach generally means you have an organized vendor management team that does the following:

- Sets guidelines
- Delegates tasks to different areas
- Monitors those tasks to completion

The vendor risk management team would ideally work very closely with the business units to ensure consistency and timeliness of practices.

With the hybrid method you have:

1. Consistency
2. Oversight
3. Proper authority
4. Contributors, which lighten the load

Now, let's jump into the bulk of third-party risk management work.

Plan and Create Governance Documents

You need well-developed governance documents in place that lay out how your program will be managed so that you can have a successful trip down the runway and launch into the rest of the third-party risk journey. We often see policy, program and procedures documentation. No matter the format type you choose, your governance documents should be reviewed and updated at least annually, but you'll also want to update them if a significant change occurs at your organization or if new regulatory guidance is announced.

By definition, **governance documentation** is a set of formalized and documented policies, standards, processes or guides that provide personnel at all levels adequate reference for how to conduct business and drive the success of your organization.

If you decide to implement third-party risk policy, program and procedures documentation as your governance documents, here's what that would look like:

1. Policy is generally a board or executive leadership set of requirements for what must be accomplished in third-party risk management as part of managing third-party risk at the organization level.

2. Procedures are step-by-step, instructional guides on how to accomplish individual tasks in order to meet third-party risk management policy and/or program requirements.

3. Programs are also very common, often in place to supplement policies and further delineate responsibilities. Programs would be more at the senior management and department head level and work as an instructive guide for how third-party risk management requirements, such as policies, should be accomplished.

Supporting/supplemental documentation to support the third-party risk management process may include:

- Flowcharts
- Checklists
- Guides/Resource Materials

Determine Oversight and Accountability

So, who's responsible for handling the oversight in these areas? Determining who'll be performing third-party oversight upfront will create better long-term results for your organization. Also, consider how the third-party risk management program will exist within the broader enterprise risk or compliance management framework.

Overall, you should consider the three different types of responsibility in your organization, sometimes referred to as the three lines of defense.

Here's a breakdown:

First Line

The first line is the line of business interacting with customers and vendors at the transaction level. They're your eyes and ears as they work with the vendor daily. So, if something isn't working well, the vendor isn't meeting service level expectations or the vendor is unresponsive, then your first line is likely going to be the first to know. The role falling into this category is typically a position like vendor manager. The first line owns and manages vendor risk.

Second Line

This would be the third-party risk management function at an organization. They're often responsible for ongoing and annual assessments, delegating responsibilities and overseeing the program, among other duties. The roles falling into this category typically include management positions within the enterprise risk or compliance departments. The second line oversees the risk.

Third Line

The internal audit department commonly reports into either compliance or enterprise risk and performs internal assessments of first and second lines of defense to ensure corporate policy and program compliance. The role falling into this category is usually an internal auditor. The third line assures that the first and second lines are sufficiently managing and overseeing vendor risk.

To get more specific, here's an overview of typical roles you would see in third-party risk management:

Regulators - A regulator is a state or federal regulatory agency tasked with being the supervising entity of a specific industry. Regulatory examiners review an organization's compliance with rules and regulations, and ensure that they operate in a safe and sound manner. They review your third-party risk management process to verify the organization is considering every aspect of the third-party risk management lifecycle. Regulators are looking for evidence of a consistently effective program.

Auditors - These can be external or internal. They identify gaps or concerns in your third-party risk management program before an examiner does. They share best practices, advice, where change is needed and more.

Executive Leadership and/or Board of Directors - Their involvement isn't just a must; it's critical. In fact, leading regulatory guidance mandates their involvement. They should especially be in the loop regarding critical and high-risk vendor activity. It should also be the board's responsibility to approve your vendor management policies and set the "tone-from-the-top."

Senior Management - Senior leaders throughout the organization should be involved in developing the process, procedures, projects and reporting infrastructure for the organization's third-party risk management program. They review the policy and assign people and responsibilities accordingly. They also ensure monitoring of fluctuating risk levels and review service level agreement (SLA) reporting to make informed decisions.

Dedicated Vendor Risk Management Team - This group helps facilitate the development of governance documentation and confirm the organization is following industry and regulatory guidelines and best practices. Often, they lead the vendor assessment process and tracking report on valuable vendor information.

Vendor Owners - Often, this is the person who is directly responsible for the vendor relationship within the line of business. They perform the daily management of the vendor.

Subject Matter Experts (SMEs) - SMEs assist with due diligence assessments, such as reviewing vendor SOC reports, financial statements, business continuity plans and more. These experts have obtained certifications that qualify them to do so (e.g., a certified public accountant (CPA) may review a financial statement or a CISA/CISSP to review information security controls). SMEs can be internal or external.

Third Parties - A company or entity with whom the organization has a direct written contract with to provide an outsourced product or service on behalf of the organization.

Fourth Parties - A company or entity with whom a third-party vendor has a direct written contract with to provide an outsourced product or service on behalf of the third-party vendor's organization.

Define Scoping

Much like you wouldn't get on a plane to travel a few miles away, not all vendors need to board the third-party risk management plane and go through all the steps. Based on that, make a determination on whether the engagement falls within or if it should be excluded from the flight path as they're out of scope.

Some examples of third parties often written out of scope include:

- Government agencies
- Utility companies
- Office supply companies

Perform Risk Assessments

Risk assessments are an important part of our third-party risk management flight path as they help you determine if the vendor is critical or non-critical to your organization and their overall risk rating. When assessing risk, it's important to address the inherent risk, residual risk and criticality of your vendors.

Criticality

Critical relates to those processes, products and services vital to your operations, revenue stream, customers and reputation. In other words, your business would be materially impacted if these activities weren't performed as expected. Of course, each organization must determine for themselves what attributes are used to define critical. Still, there are some customary qualifying conditions to help you identify your critical third-party vendors more effectively.

A good rule of thumb is to ask these three questions:

1. Would the sudden loss of this third party cause a significant disruption to your business?
2. Would the disruption impact your customers?
3. If the vendor service is disrupted, would there be a negative impact on your operations if the time to restore service took more than 24 hours?

Depending on your organization, other factors may also be considered as you identify your critical third-party vendors. Here are some examples of considerations:

1. Are significant financial investments, resources and time required to implement the third-party relationship and manage the risk?
2. Would there be a material impact to the organization's operations or resources to engage an alternate third party or if the outsourced activity has to be brought in-house?
3. Could the third-party vendor failure attract regulatory scrutiny or result in enforcement actions, including fines?
4. Could the third-party vendor failure negatively impact your reputation and brand?

Inherent Risk

Think of inherent risk as a "first impression." It's the amount of risk a vendor poses to your organization simply based on the nature of the relationship. This means, risk that is present before action is taken to manage it through mitigation. To determine the inherent risk, you likely should have to go to the vendor for lots of information. Anyone bringing on a new vendor internally should be aware of the nature of services enough to make this determination.

The following are examples of inherent risk assessment questions that you may want to ask:

- Does the vendor or product align with our strategic goals?
- Does this product or service in any way impact our clients and/or customers?
- Is sensitive data being accessed by this vendor?
- Does the vendor process financial transactions on our behalf?
- Do we rely on this product or service in order to maintain compliance with any regulatory guidance?

Mitigation

After you've determined the criticality and inherent risk rating, document each risk thoroughly and pinpoint the appropriate steps for each. What you learn here will both help protect your organization and inform the depth of due diligence and ongoing monitoring needed.

Now, the next step is evaluating any mitigating controls, or in other words, what steps can be taken to address or mitigate the risks. In order to accurately determine residual risk, you'll need to collect the appropriate documentation from your vendors which you will also need to review for assurance around controls. More detail around the documentation to collect is covered in the due diligence section of this eBook.

Residual Risk

After you've conducted due diligence to assess how certain measures affect the existing, inherent risk, you can then determine the residual, or remaining, risk. Residual risk should never be higher than inherent risk. Practically speaking, it should always be equal to or perhaps less than the inherent risk level.

PRO TIP
If you think the residual risk may be higher than the inherent risk, there's a good chance you've misidentified some elements of the inherent risk.

Other Risk Categories

There are several other ways that risk can be categorized. Many of these other risk categories overlap, but it's still helpful to understand how they affect your overall vendor risk assessments. Additionally, some industries require categories of risk to be evaluated specifically, while others do not.

Categories of risk often include:

1. Strategic. Strategic risk occurs when a prospective or current third-party vendor's decisions and actions are incompatible with your organization's strategic objectives.

2. Reputational. Reputation risk encompasses any of the numerous ways your third-party vendor could directly or indirectly damage your reputation, brand or organization's name. This harm could result from their actions, poor service, lawsuits, outages, fraud or data breaches.

3. Operational. Operational risk has two components, internal and external. Internal operational risk is broadly defined as the risk of loss resulting from a third-party vendor's ineffective or failed internal processes, people, controls or systems. Internal operational risk is specific to how things are accomplished within an organization vs. risks inherent within a particular industry. Internal operational risk is directly influenced by people.

4. Financial and Credit. Financial and credit risk directly relates to the financial condition of the third party itself. Suppose the third-party vendor has insufficient investor funding, cash or credit available to meet their contractual obligations. In that case, there is a risk they won't be able to provide products and services to your organization.

5. Compliance. Compliance risk arises from a third-party vendor's failure to comply with laws and regulations governing the products and services your organization provides to its customers. Compliance risk is also possible when your third-party vendor doesn't follow your internal policies, procedures, business standards or conduct codes.

6. Third-Party Vendor Cyber Risk. Third-party vendor cyber risk stems from third-party vendor security vulnerabilities. Two of the most common cyber risks resulting from missing or ineffective controls are cyberattacks and data breaches.

7. Other. The categories of risk aren't only limited to the ones previously mentioned. Other risks such as concentration, geo-political, sustainability or environmental, transaction and more can be present.

Once your risk assessment is completed, further action may be necessary, depending on your results:

- Do you need to implement additional controls to further mitigate the inherent risk?
- Do you need to increase your level of due diligence and oversight?
- Are there items you need to address in the contract?

Communication and collaboration are instrumental in implementing a consistent risk assessment process. Each area requires attention from various levels of expertise, so leverage your internal resources to assist with the risk assessment process.

Do Your Due Diligence

Collecting vendor due diligence is one of the most arduous components of third-party risk management with all its seemingly never-ending checklists. In some ways, it's a bit like one big game of tag — constant calls, emails, etc. all just to get a few pieces of necessary documentation.

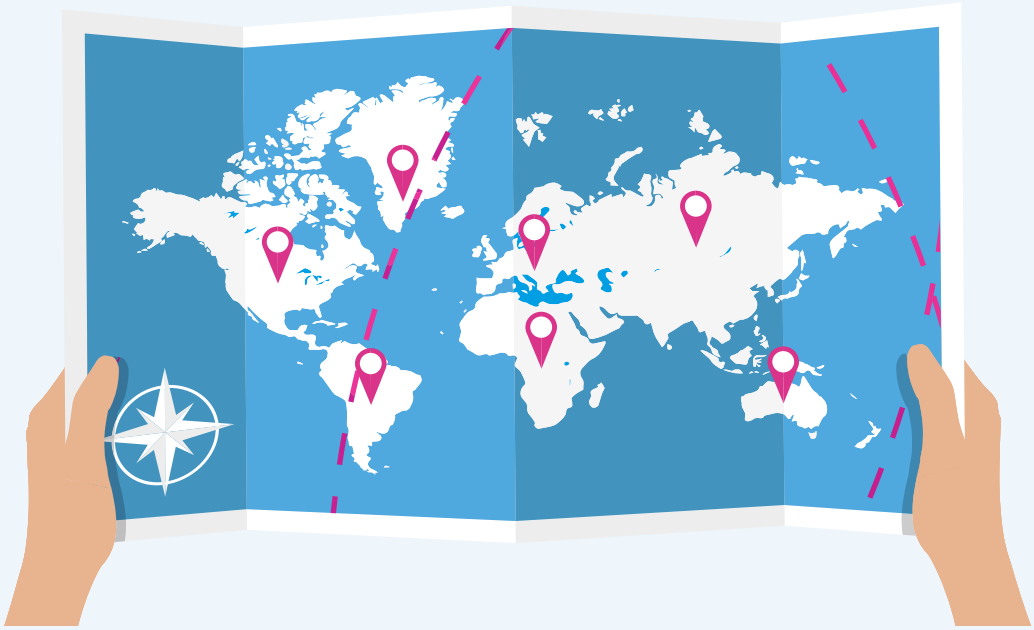
Then there's the effort required to fully assess these documents. Sometimes, it's difficult to determine where to begin, what needs to be reviewed and how to interpret the data properly.

Here are a few helpful steps for properly handling vendor due diligence:

STEP 1

Review Your Contracts

Aside from conducting a contract review before it's up for renewal, and especially if those conducting due diligence aren't the same folks who manage the contract, the first thing you should do when initiating a due diligence assessment is review the contract for anything that might be pertinent to your risk assessment. Are there specific security parameters that should be in place? Are they held to providing you any particular documents? Is your organization supposed to be incorporated into their business continuity plan? Are there specific recovery time objectives (RTOs) that need to be validated? It's good to have a general understanding of what is and isn't in the contract before initiating your due diligence request.



STEP 2

Collect and Review Vendor Data.

Use what you know about a vendor's services and inherent risk to determine what measures should be in place to mitigate that risk. For the most part, you want to validate a vendor's overall good standing, and ensure that they're able to provide the expected services with the same level of security, compliance and business ethics as would be expected internally. Here is a baseline list of items which may help in providing the assurance collected and/or reviewed as part of the due diligence process:

For any vendor to provide and/or your organization to research and obtain the following:

- Basic Information (Full Legal Name, Address, All Physical Locations, Website URL)
- Secretary of State Check
- Ownership structure and affiliated companies OFAC/PEP checks
- Certificate of Good Standing
- State of Incorporation
- Dun & Bradstreet (D&B) report
- Vendor negative news search findings
- Picture or Google map view of facility (if required)
- Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- Business license
- Tax ID
- Any “doing business as” or “also/previously known as” (d/b/a, aka, pka)
- Vendor complaints research findings
- List of subcontractors/fourth parties
- Credit report
- Articles of Incorporation
- Conduct check of CFPB Complaint Database and/or Better Business Bureau rating

Additional considerations for critical vendors or elevated inherent risk

If the nature of services requires a little more validation than your standard background check, you'll want to expand your initial request for information to include more detail around their internal practices. This could be by way of completing custom or standardized questionnaires, sending their policies or procedures or providing existing reports or certifications. Remember, every vendor's control environment is different, and so is the nature of each of your vendor engagements.

Here are some examples:

- Internal policies and/or procedures
- Audited financial statements or the most recent financial statements
- SOC audit reports
- Business continuity, disaster recovery and pandemic plans and testing results
- Completion of a questionnaire for any additional information needed to understand risk exposure or mitigation

So, while no two due diligence assessments will be the same, there are some common control areas and documents you'll want to be familiar with and know how to review.

Let's cover four of them in more detail:

1. Vendor SOC Reports.

SOC stands for system and organization controls. It's an independent audit report performed by a certified public accountant (CPA) that shares additional details around the vendor's controls in place. It's an attestation that your vendor controls to safeguard your data, and if the safeguards are operational, they would effectively mitigate part of the risk inherited by using the vendor.

To help you with conducting a SOC review, from a high-level, you'll want to:

- Use the reporting period to confirm it's the most current report available
- Assess organizational and administrative set up
- Confirm products and services
- Gain a deeper knowledge of the information system
- Review data center infrastructure
- Analyze control objectives and activities
- Review any audit findings, or control exceptions and how management responded

2. Business Continuity, Disaster Recovery & Pandemic Plans.
Business continuity planning assists vendors (or any business) in ensuring that their significant operations and products/services continue to be delivered in a full, or at a predetermined and accepted, level of availability. The expected level of availability is typically outlined in the service level agreement (SLA) that your organization has with the vendors.

When conducting due diligence around business continuity plans, make sure the vendor has a formal plan that accounts for:

- Strategy for personnel loss
- Pandemic contingencies
- Relocation plans
- Breach/notification policy
- Business continuity impact analysis
- Recovery time objectives
- Recovery point objectives
- Data around testing and ongoing maintenance of the plan

The vendor should also consider pandemic planning, which focuses on:

- Strategies and procedures in the event of a pandemic
- Preventative measures
- Implementation guidelines in the event of a prolonged health crisis

And, a disaster recovery plan, which primarily focuses on systems as well as:

- Gathering of disaster recovery personnel at the command center
- How the vendor will decide if the incident is a disaster
- Salvage operations, recovery operations, communications and restoration to normal operations

3. Cybersecurity Posture.
A cybersecurity program helps protect your organization and the vendor from potential vulnerabilities like a data breach. Evaluating your vendor's cybersecurity posture will help you identify potential weaknesses. From there, you can effectively communicate with the vendor about those weaknesses and develop strategies to strengthen controls prior to a breach happening.

- Security testing (vulnerability, penetration and social engineering)
- Sensitive data security
- Data retention/destruction, declassification and privacy policies
- Employee, contractor and vendor management team data protection training (e.g., annual security training, access management policies)
- Incident response plan

4. Financials.
Financial statements should be reviewed to identify the financial health of any vendor you outsource a product or service to. This helps you determine if the vendor can continue to provide secure, safe and quality products or services that meet your organization's expectations.
Make sure to determine/review:

- If the vendor is a public or private company so that you know what report type to request
- If regulatory action has been taken
- If there are outstanding legal proceedings or lawsuits associated with the vendor
- The vendor's net worth (balance sheet)
- Revenue and gross margin (income statement)
- How the vendor funds operations (cash flow statement)
- Likelihood of bankruptcy (ratios)

STEP 3

Determine Current Residual Risk

Now that you've determined the inherent risk and requested and assessed vendor due diligence to further evaluate their control environment, you can determine the residual risk. Again, this is the remaining risk present once all efforts to control, or mitigate, the inherent risk has been made. Remember, mitigating risk isn't completely the vendor's responsibility. You may want to consider what your organization is also doing internally to mitigate risk associated with a relationship to get a better gauge of true residual risk.

While many organizations have found various ways to quantify the calculation of residual risk, it's often a very subjective rating, and must incorporate a broad understanding of all factors associated with a vendor relationship.

STEP 4

Escalate Issues or Concerns

If there are still major issues or concerns, it may be time to escalate. Escalate these concerns to senior management and/or the board as needed to keep them in the loop. Also, create a methodology to track these issues or concerns.

The process often looks like this:

1. You've identified the issue and determined the severity

2. You notify the correct departments and teams who need to help with managing the issue(s)

3. Track the issue through remediation to ensure it's resolved properly (e.g., determine an action plan, keep a conversation log)

Consider Fourth Parties as Needed

Sometimes, there may be a need to dive a little deeper into the matrix of your vendor environment and assess your vendors' vendors, which are your fourth parties. Like you, your vendors are deeply reliant on some of their vendors, and these are the ones you need to concern yourself with under two main circumstances:

- The fourth party has access to your data
- The fourth party provides critical services to your third party

These vendors should be the ones to show up in your third parties' SOC reports and should also be easily identified by your vendor as those classified as critical in their own vendor management matrix.

The SSAE 18 Report
Thankfully, with the introduction of the SSAE 18 report in May 2017, your third-party vendors are now required to identify their significant vendors aka your fourth parties. This makes it much easier for you to know which fourth-party vendors you should actively monitor.

You need to understand the following three things about these significant fourth-party vendors:

1. Who they are
2. What products and services they provide to your vendor that cause them to be classified as critical to their operations
3. What your vendor has done as part of their due diligence on these vendors

How to Get Information on Fourth Parties

Ask your third-party vendor to provide you the following pieces of information:

- A copy of their own vendor management policy
- A complete list of all vendors they classified as critical and/or high risk
- Ask for a complete list of their vendors who may at any point have access to your data or who are essential in your third party's ability to provide services to you
- The fourth-party vendor's SOC report (your third-party vendor can typically get you a copy of it, but you'll need to sign the fourth-party vendor's confidentiality agreement)

Once you have this information, review it and formulate your opinions of the risk these fourth-party vendors pose to you (not your third-party vendor). If needed, ask additional questions to ensure you understand the products or services being provided and how they can impact you.

Where Fourth-Party Vendors Pose Risk to You

Here are a few common areas where a fourth-party vendor may pose a risk to you:

- Your sensitive data is being transmitted or stored by a fourth-party vendor and could be exposed if the vendor's system is breached

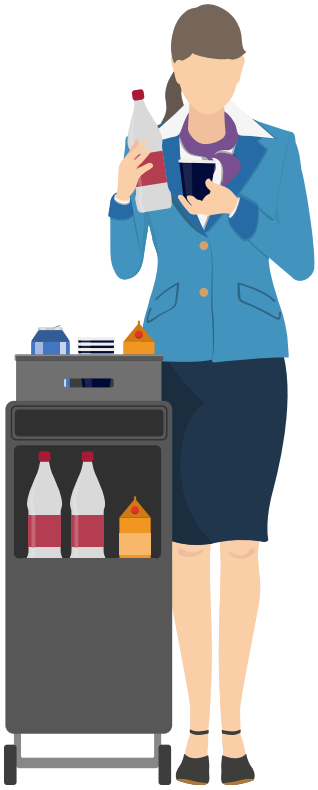
- Payment processing or other dependent services for your own customers may fail if the fourth-party vendor experiences a failure

- Downtime of the fourth-party vendor may be visible to your own customers depending on the integration method

> **NOTE**
> *As a rule, you don't need to be concerned about fourth parties who pose incidental risk (e.g., the third party's vending machine company).*

Select Appropriate Vendors

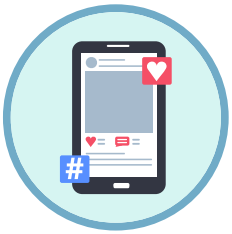
You may be wondering why we're just now discussing vendor selection. This is because the ultimate decision to engage with a third party should only be done after sufficient due diligence has been completed and the residual risk has been identified. Having a thorough and well-defined process for selecting a new vendor is critical to the success of the long-term relationship. You must research potential vendors and perform adequate due diligence to confirm they meet your operational and strategic objectives. A key asset in conducting this research would be to issue a Request for Proposal (RFP). An RFP is a document that's shared during vendor selection with a group of vendors under consideration, or could be published on your organization's website, as an attempt to find the best vendor to meet your organization's specific business needs. If you choose to not distribute an RFP, you still want to speak with multiple vendors in the market space and do your risk-based due diligence.



Once you've decided if you're going to issue an RFP or not, it's time to begin to compare your potential vendors by listing out the pros and cons of each.

Some ways to help you do this include the following:

Check for any customer reviews or negative news about the potential vendors



Scan their social media sites, set up Google News alerts and research complaints through sites like ripoffreport.com, the Better Business Bureau and the Consumer Financial Protection Bureau (CFPB) public complaints database

Create a standard due diligence checklist to use when vetting vendors and tailor it further based on the product or service type

Complete at least one inherent risk assessment on each vendor

Remember, due diligence is one of the most important activities in third-party risk management, so do your homework. What do you need to know about the vendor before you enter into a business arrangement? What due diligence do you need to continue to perform on them due to the nature of the vendor relationship?

Perform Adequate Contract Management

If you've completed due diligence and a risk assessment and have narrowed down a vendor you'd like to contract with, you need to consider contract management. 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:

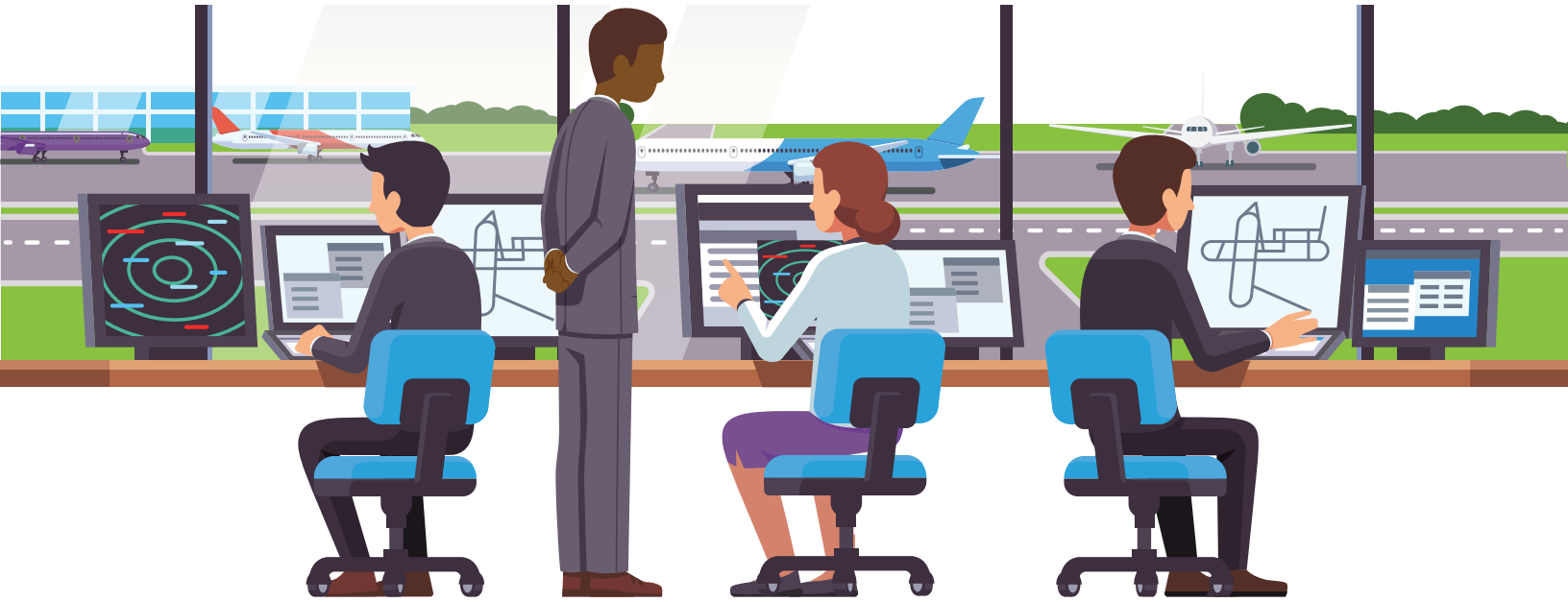
1. Go in thinking about the entire lifecycle of the third party.

2. Determine what you may need from the vendor along the way and already be thinking about your exit strategy should the relationship terminate (because it happens!).

3. Get it into the contract! If you have specific requests, for example documents that should always be provided or a request that the vendor notify you of a data breach in a certain timeframe, then write it into the contract.

4. Be sure to centralize and standardize your contract process.

PRO TIP
Remember that you have the most leverage over a vendor before you sign the contract, so carefully consider the terms and provisions.



Here are three reasons why vendor contract management is important:

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 the old saying, "if it isn't in the contract, it won't happen," is truer than ever.

3. You, the organization, are held responsible for any issues discovered post-contract execution – yikes! It's an expectation that you've conducted adequate due diligence with your applicable industry regulations and expectations in consideration prior to signing the dotted line.

There are 14 major elements you should be considering when implementing your contractual standards. These include:

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
14. Business Resumption and Contingency Plans

Service Level Agreements

When thinking about contracts, another important element to consider is if a service level agreement (SLA) should be included or not. SLAs focus on performance measuring and service quality agreed to by your organization and the vendor and may be used as a measurement tool as part of the contract or as a stand-alone document.

Your SLAs should state the following:

- Metrics
- Responsibilities
- Expectations
- Timing and Frequency

PRO TIP
Most SLAs favor the vendor, as they begin with standard service levels that are provided by them. No matter what the vendor initially states, don't take these terms as non-negotiable. Instead, these should be viewed as a good starting point for negotiation.

Report on Vendor Risks

A major component to good communication is having sound and consistent reporting of vendor risk information. No matter your corporate structure, there are always various departments and stakeholders that need to understand vendor risks, especially as they might affect the organization as a whole. A wide range of third-party risk management activities must be documented, tracked and reported to the right people. It's a fundamental requirement to keep your senior management team and the board informed of any issues that may arise, and without proper tracking, it would be a challenge to provide the necessary details. Furthermore, the board and/or executive leadership must have an adequate understanding of the vendor risk environment in order to accept and approve of all the risk taken on by an organization.

Create standardized reports and, when needed, customize reports. In addition, be sure to establish a frequency of when you'll cover the information. Also, be sure that documentation and reports for the board are crisp, clean and easy to follow.

PRO TIP
The ideal reporting frequency is monthly to a risk committee and quarterly to the board.

These are the SEVEN reports you should always have on file regarding your third parties:

1. Overall inventory (e.g., actively managed vendors, percentages of critical and non-critical vendors, etc.)

2. New regulatory requirements (e.g., any that require changes to governance documents)

3. Due diligence and vendor selection (e.g., status of current and ongoing vendor selection processes)

4. Risk assessments (e.g., number of vendors with risk assessments completed, significant changes)

5. Vendor risk issues (e.g., concerns with a contract, vendor isn't meeting SLA performance)

6. Reporting timeline (e.g., timeline of the reports and meetings for the lines of business)

7. Industry highlights (e.g., big news headlines like vendor announcements, vendor data breaches)

Continuously Monitor and Assess Vendor Due Diligence

In addition to running reports to analyze performance, you'll want to perform ongoing monitoring and oversight. This is extremely important to do. It's important to keep an eye on your vendors after you sign a contract to ensure you're remaining aware of any new risk posed.

Ongoing monitoring includes:

- SLA tracking and monitoring
- Staying abreast of any issues or changes
- Periodic risk assessments

Ongoing Monitoring Best Practices

1. Set up SLA tracking
SLA tracking is critical to understanding how a vendor is performing, so be sure to set up a method, possibly in a platform, to track these metrics.

2. Use an open-source monitoring tool
This should give notifications on significant vendors throughout the engagement.

3. Base review schedules on inherent risk
If a vendor is inherently high risk, but moderate residual risk, you'll want to review on a high-risk frequency.

4. Set an ongoing monitoring standard
It should make sense for your organization and resources. However, a general rule of thumb would be critical and high risk annually, moderate risk every 18 months to two years and low risk every two or three years.

5. Stick to your internal third-party risk management policy
Examiners will want to see to that work product matches this.

Periodically Perform Independent Reviews

Sometimes, your third line of defense, which is internal audit, will need to review your third-party risk management program to help with identifying any gaps and discrepancies in the process (they should be doing this at least annually). When they identify gap and discrepancies, you should address and resolve them. This early involvement helps immensely with your exam and audit prep. This will be happening periodically as vendors are going through your third-party risk management flight path.

Consider Termination in Advance

Often, there comes a time where an engagement must come to an end and some vendors to deplane. This can occur for several reasons:

- Vendor's failure to perform
- Contract term is up
- A better vendor option is available
- Cutting costs

There should always be some consideration into how the termination processes may look for any particular vendor.

In some cases, once a contract term has come to an end, not much needs to be done besides removing the vendor from inventory. For more significant or critical vendors, you'll need to follow your exit strategy and be sure you're terminating the relationship in accordance with contracted terms that you laid out in the contracting stage.

Exit Strategy Considerations

When crafting a good exit strategy, you'll want to take the following actions:

1. Discuss the exit strategy with the people in your organization who are the experts on what to do. In some cases, the exit strategy may be as simple as switching vendors.

2. Write out a detailed timeline of what would need to happen to minimize disruption to your business and your customers if something happened to the vendor which would impact your operations.

3. Consider all of the alternatives, whether it would be a slow unwind or a hasty plan that can quickly be put in place.

4. Have it reviewed and, if possible, tested and even potentially included in your vendor's contract.

5. Review the exit strategy periodically with those same subject matter experts to be certain it's accurate and detailed enough.

Stay Educated

Third-party risk management is a constantly changing and evolving space, so there's so much to know and learn. As a professional in the industry, it's crucial you stay informed. Here are some ways you can do that:

1. Attend industry events such as conferences and webinars. There are a lot of free webinars out there! Track and take credit for the investment of time and money in ongoing education. Be sure to keep your senior management team and the board informed and well-educated, too.

2. Read industry news and resources such as infographics, eBooks, whitepapers and more.

3. Set up Google News alerts that focus on keywords, topics, your vendors and anything else that you want to remain current on.

4. Read and understand the regulatory guidance - both current and any new or updated guidance announced.

5. Review enforcement actions and consumer complaints as these help you better understand what not to do (paymentlawadvisor.com and the CFPB complaint database are helpful sites).

There's a lot to know, but keep in mind this important advice: third-party risk management isn't a one-and-done activity. It's a recurring process with due diligence and risk assessment updates on a regular basis to prevent a lot of turbulence.

As you're working on getting from one destination to the next and ensure that you get there successfully, a good grasp on how to navigate through these third-party risk terminals will help your organization, your customers and your key stakeholders remain safe on the third-party risk trip.

Download free samples of control assessments and see how Venminder can help reduce your third-party risk management workload.

Download Now

venminder

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

(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 library. The assessments enable clients 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.