31 Third-Party Risk Management Best Practices *in 2024*

venminder

01

Know the laws, rules, and regulatory guidance for your industry.

The June 2023 release of the Interagency Guidance on Third-Party Relationships: Risk Management was a significant reminder that regulators are increasing their focus on third-party risk management. Even if your organization isn't regulated by the three agencies (FDIC, OCC, and the Fed), consider other recent regulations such as the FTC Safeguards Rule, the SEC Breach Notification Rule, and the NCUA Cyber Incident Notification Requirements. It's important to identify, read, and understand all regulatory guidance, laws, and rules that apply to your industry. These guidelines are often considered best practices that will ensure safe and sound third-party relationships. Make sure to do research and consult with your compliance department with any questions.

02

Establish clear roles and responsibilities.

Third-party risk management programs are most effective when stakeholders understand and fulfill their responsibilities. For example, do your vendor owners know they're responsible for identifying vendor risk at the beginning of the engagement and throughout the relationship? Does your senior management understand the roles of the third-party risk management team vs compliance or the lines of business? Make sure the roles and responsibilities are clearly defined in your policy, other governance documents, and training materials. Don't forget to include those roles that provide oversight and governance.

03

Define which third parties are in scope for your program.

Organizations that must comply with the Interagency Guidance should understand that any third-party business arrangement, with or without a contract, is in scope for third-party risk management. Organizations that aren't subject to the regulation will need to make this determination for themselves. Typically, your program should include those third parties providing products or services to your organization or its customers on your behalf.

However, some third parties providing products or services, such as public utility companies and media subscriptions, are commonly excluded from most third-party risk management programs. Other vendors, such as rating agencies or external auditors, would also be out of scope.

Several product categories can be safely excluded. Media subscriptions, sponsorships, donations, and memberships and conferences in industry groups are examples of out-of-scope relationships. No matter who is in or out of scope, make sure you can articulate and justify your decisions for auditors and regulatory examiners.

04

Ensure you have a well-written policy and other governance documents.

Your policy is the foundation of your third-party risk management program and is the document that formalizes your third-party risk management requirements for all organizational stakeholders. It should clearly outline the rules and requirements of the program, roles and responsibilities, and oversight and governance. Regulators and auditors will want to see that the policy reflects the current state of your program, so it's important to keep it accurate, even if there are improvements to be made in the future. It should also be easily accessible to all employees.

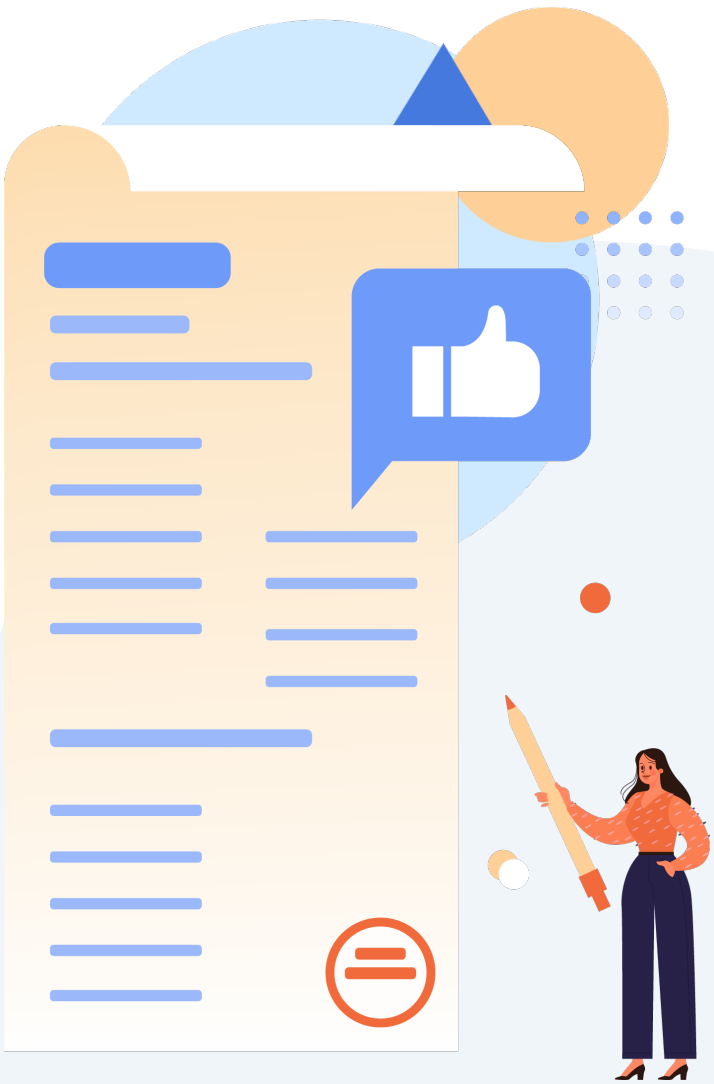
Beyond your policy, a program document can provide details about the specific processes used to meet the policy's requirements. A program document is also an excellent resource for senior management and other stakeholders to learn more about the elements of your third-party risk management framework and how they fit together. Your program document should describe your current third-party risk management roles and responsibilities, workflows, approvals and exceptions, timebound activities, quality expectations, and oversight and governance.

Detailed, step-by-step procedures enable your stakeholders to execute third-party risk management processes. The best procedures address one process at a time and are stakeholder specific and are written in such a way that anyone can follow them and generate the same output.

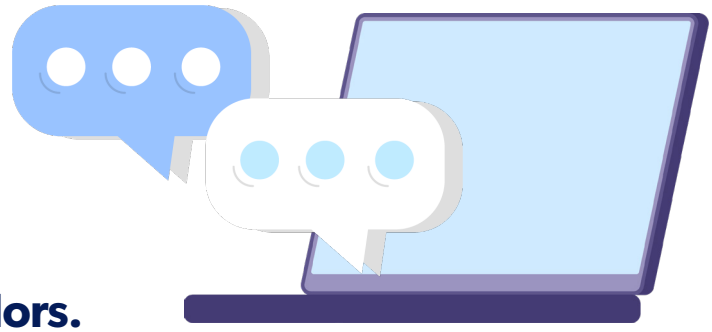
05

Review and update your policy annually.

Regulatory requirements and best practices dictate that third-party risk management policies should be reviewed annually and updated if necessary. This ensures your policy reflects the most up-to-date regulatory guidance and represents your current third-party risk management activities and processes. Your board should review and approve the policy annually. If your organization doesn't have a board, then policy approval is the responsibility of senior management.



06



Define the criteria for critical vendors.

Your organization must identify the vendors most essential to its day-to-day operations or that provide vital services to your customers. Not only do auditors and regulators focus on these critical relationships, but it's necessary to incorporate them into your internal business continuity planning and testing. Critical activities and operational resilience are common themes that have been highlighted in regulatory guidance, such as the Interagency Guidance and the EU's Digital Operational Resilience Act (DORA), as well as publications from the OCC, SEC, FDIC, and NCUA. Your critical vendors should represent a very small subset of your total vendor inventory and should be limited to those that can affect your business on an enterprise-wide basis, as opposed to a specific business line.

Who defines what is essential? How do you know if your vendor is truly critical vs important? Defining the specific critical vendor criteria is necessary to avoid confusion in your organization.

TO BEGIN, ASK THESE THREE QUESTIONS:

- Would the sudden loss of this vendor cause a significant disruption to our organization?
- Would that disruption impact our customers?
- If the time to restore service exceeds 24 hours, would there be a negative impact on our organization?

If you answer yes to any of these three questions, you're likely dealing with a critical vendor.

Remember, the term "critical" shouldn't be used as a risk rating, but rather as a way to identify that small subset of vendors that pose the greatest operational impact to your organization should they fail.

Make sure you define critical vendors' criteria and memorialize them in your policy, other governance documents, and training materials.

07

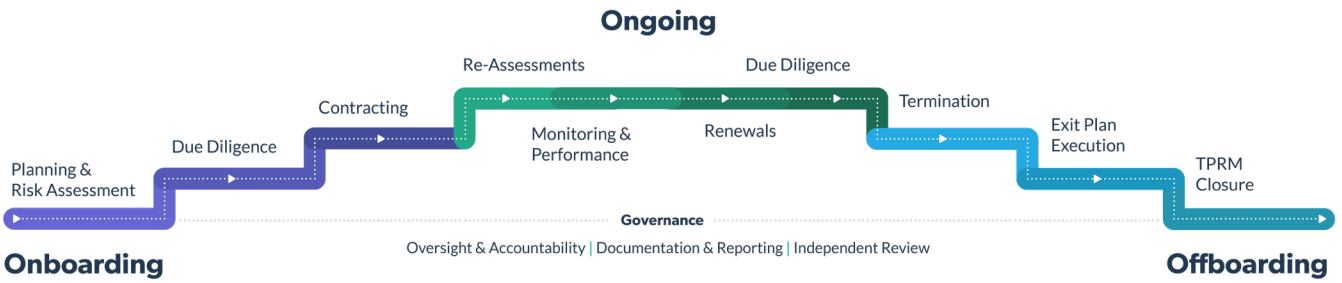
Use a risk-based approach for all third-party risk management requirements and activities.

Third-party risk management activities should always be proportionate to the risk and criticality of the vendor engagement. That means high-risk and critical vendors will require more robust and thorough due diligence, monitoring, and contracting activities. The Interagency Guidance also advocates for this approach by stating that not all third-party relationships will require the same level of oversight or risk management. Each vendor is different and brings their own unique combination of risk to the table. With a risk-based approach, you can allocate your resources more efficiently and concentrate on the vendors and risks that pose the greatest threat.

08

Follow the third-party risk management lifecycle.

The linear third-party risk management lifecycle is a user-friendly adaptation of the circular lifecycle that was originally developed by regulators. The lifecycle presents a scalable, easy-to-follow methodology that has become a best practice across all industries. The lifecycle is the perfect roadmap to guide your organization through all the necessary steps and activities required to effectively manage your vendor relationships.



THE LIFECYCLE IS DIVIDED INTO THREE STAGES: onboarding, ongoing, and offboarding. Each stage has required activities, which must be performed in a specific order:

ONBOARDING begins when your organization identifies the business need for a new vendor. You must plan for the relationship, identify a vendor owner, and establish an exit strategy for the relationship's conclusion. Then it's time to assess the inherent risks of the product or service (and vendor relationship) to establish a risk rating for the engagement.

Next, assess whether the product or service will be critical to your business or customers. After identifying risk and criticality, you can scope vendor due diligence, issue a vendor risk questionnaire, and collect documentation about the vendor's risk practices and controls. Subject matter experts (SMEs) review the vendor's due diligence information and determine if the vendor's controls are appropriate and can effectively mitigate the known risks.

After successfully completing due diligence, you can address any issues or findings with the vendor or decide to decline the relationship. If you choose to move forward with the vendor, it's time to negotiate and execute the contract. Once the contract is signed, the vendor relationship moves to the ongoing stage.

ONGOING risk re-assessments, management, and monitoring are important activities in the ongoing stage. A risk-based schedule is used to re-evaluate risks and perform due diligence, with the highest-risk engagements re-assessed more frequently. In addition to periodic formal reviews, continuous monitoring and management of risk and performance are essential. Contract review and renewal (when applicable) are also integral to the ongoing stage.

OFFBOARDING requires notifying the vendor of your intention not to renew the contract or terminate the contract early. Once notification has been received, you must execute your exit plan. The plan should detail all the roles and responsibilities of both parties as well as account for essential activities, such as the return or destruction of confidential data, de-provisioning vendor access to your data, systems, and facilities, and return of physical assets and intellectual property. When all the necessary activities are completed, it's time to review and pay final invoices and update all systems to reflect the vendor's status. All documentation must be properly organized and stored and should be easily accessible if needed for an audit or regulatory exam.

09

Assign a vendor owner for every vendor risk engagement.

Every vendor relationship needs an identified owner. These relationship owners are often called vendor owners, vendor managers, or product owners. They're responsible for the product or service the vendor provides to the organization. To do this, they're responsible for identifying, managing, and monitoring vendor risk throughout the relationship and regularly work with the vendor, enabling them to identify risks or issues early on before they become larger problems.

Vendor owners must abide by the rules and requirements of the third-party risk management program. The best vendor owners have a strong understanding of the product or service provided and have enough skill and bandwidth to manage the vendor relationship.

10

Identify your exit strategy early.

As soon as you identify a potential vendor, you'll also need to consider what your organization will do if that vendor relationship doesn't work out. Would you switch to another vendor? Move the work in-house? Would you discontinue the product or service altogether? Having a documented exit strategy is part of planning for the relationship and ensures your organization is prepared to act if necessary. It's also a best practice to review the exit strategy periodically to ensure it's still realistic and achievable.

EXAMPLE

Suppose your strategy involves moving the product or service to another vendor. In that case, you'll want to periodically confirm the replacement vendor is still in business and has the desire and capacity to service your organization. Or perhaps there are new vendor options not considered previously. In any case, reviewing the exit strategy for high-risk and critical vendors is recommended at least annually.

11

Build your exit plan during onboarding.

For your high-risk and critical relationships, it's important to have a documented plan detailing how you will execute the exit strategy. An exit plan should outline the roles and responsibilities of both parties, tollgates or approvals, communication plans, and contingency plans if the vendor fails to fulfill their obligations.

The best time to build your exit plan is during onboarding. This is when your organization takes the necessary steps to bring your vendor to a business-as-usual state, so it's the perfect time to consider each of those steps and how you would need to reverse them when exiting the vendor relationship.

If you wait to build your exit plan until the actual offboarding process, you risk missing important steps or miscalculating the timing necessary to perform specific actions. Offboarding can be stressful, especially if it's unplanned. Without a well-thought-out exit plan, serious risks are more likely to go unidentified or unmanaged when time is short, and pressures are high.

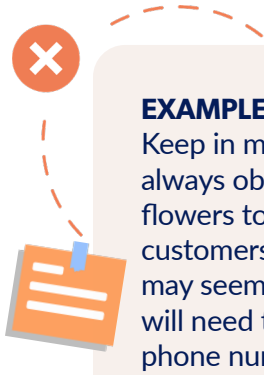
EXAMPLE
Suppose your vendor requires access to three of your internal systems. Your exit plan can detail removing access for those three systems. Or maybe one of your business lines depends on a specific data report from the vendor. Your exit plan should account for all inputs and outputs, both upstream and downstream, and ensure they're properly re-aligned with the new vendor or internal processes. Vendor onboarding is the perfect time to capture the details you will need to offboard the vendor.

12

Assess risk for every vendor engagement.

Regardless of the product or services provided, all vendor engagements should be risk assessed using the same standardized inherent risk assessment process. Risk assessing every engagement must be a requirement, whether the vendor provides one or multiple products or services to your organization.

Your vendor's risk rating should default to the same rating as their highest-rated engagement. Suppose your vendor provides two moderate and one high-risk product or service. In that case, the vendor's risk rating should be high. This approach will ensure risk identification, assessment, management, and monitoring activities are calibrated to the highest risks.



EXAMPLE
Keep in mind that third-party risks aren't always obvious. Let's say a florist delivers flowers to an organization's high-value customers on their birthday. While flowers may seem relatively low risk, the florist will need the customer's name, address, phone number, and birthdate to deliver the flowers. This list also identifies them as "high-value" customers of a specific financial institution.

Those details are considered personally identifiable information (PII), which means the florist must have sufficient information security and privacy protection practices to protect the customer's data. In the absence of the inherent risk assessment, the florist may have been confused with a low-risk vendor when actually they pose a moderate (or even a high) risk.

13

Scope your due diligence based on the risks identified in the inherent risk assessment.

Due diligence is one of the most important activities in third-party risk management. However, it's not practical to subject every vendor engagement to the same due diligence requirements. Your due diligence should be scaled to reflect the identified risks. The higher the risk, the more comprehensive and robust due diligence must be.

EXAMPLE
Requesting a cybersecurity policy for a vendor who sells office supplies is unnecessary if they don't access, transmit, process, or store PII. Likewise, asking for a business continuity plan and testing results for a low-risk, non-critical vendor wastes everyone's time. Make sure that due diligence scope and requirements are standardized based on the level of risks. This approach saves valuable time and energy and lets you focus on the real threats and most serious third-party risks.

14

Review your vendor's third-party risk management practices.

These days, almost all organizations outsource at least some products and services. Your vendors are no different. So, do you know how your vendors identify and vet their vendors? Are you sure appropriate due diligence has occurred before your vendor executes a contract and enters a business relationship? How do they monitor and manage their vendor's risk and performance?

While it's possible to outsource products and services, it's not possible to outsource their risks. Even though your organization has no direct relationship with your vendor's vendors (your fourth and nth parties), it can still be held responsible for their actions or failed risk management. This is why examining and understanding your vendors' third-party risk management practices is imperative, especially when they provide high-risk or critical products or services. This means ensuring adequate risk identification and assessment practices and properly monitoring and managing their vendors. Take time during your due diligence process to investigate the third-party risk management practices of your vendors and re-review them periodically.

15

Require your vendor to disclose critical fourth parties.

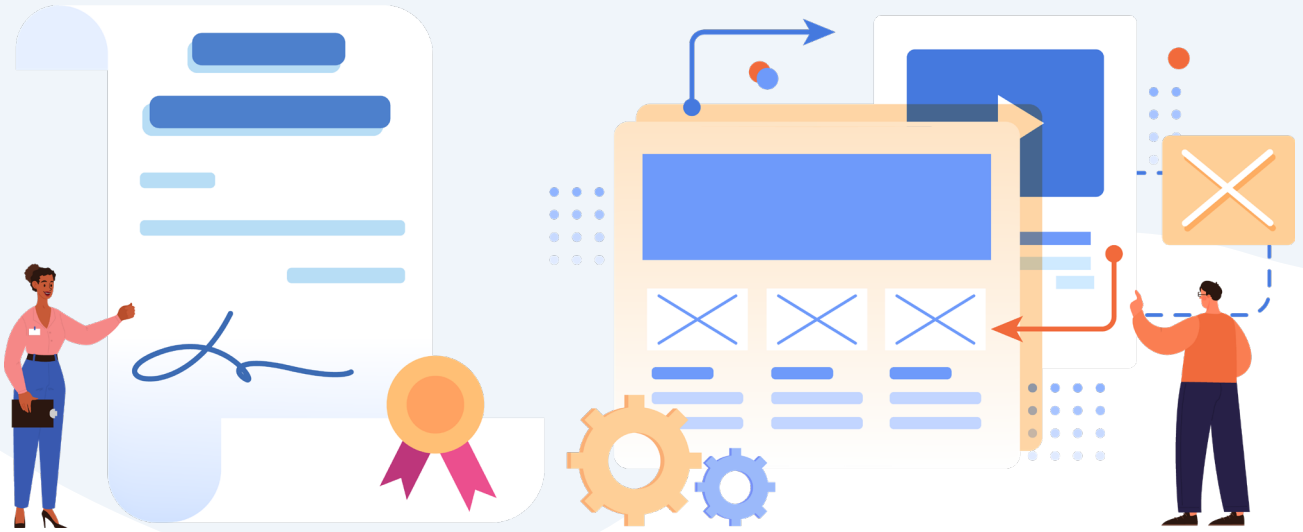
Certain fourth parties can impact the delivery of products and services to your organization if they're critical to your vendors' operations. You should make it a practice to have your vendors disclose any fourth parties vital to their ability to deliver products or services to your organization. This is especially important for vendors who provide high-risk or critical products and services to your organization. Risk intelligence tools can provide visibility to the risks of fourth or nth parties and help your organization monitor and manage those risks. Once those essential fourth parties are identified, ensure your vendor has sufficient third-party risk management processes (See item 14).

16

Use qualified subject matter experts (SMEs) for vendor risk reviews.

Reviewing a vendor's risk management practices and controls often requires significant skill and expertise. For example, one must have an in-depth understanding of the current risks to review the highly technical controls used to mitigate cybersecurity risks and how those controls work together to create a secure cyber environment. They must also discern if the vendor's controls are sufficient to protect the organization and its customers. This knowledge often results from years of specialized training and practical experience.

Organizations should place a high value on and have strong confidence in their internal and external SMEs. This is why SMEs should have professional credentials and certifications in their risk domain. The vendor risk review serves as the tollgate for a go or no-go decision to formally enter a business relationship with the vendor. The organization and its customers can suffer if the vendor risk review isn't conducted by a qualified expert. Don't take chances. Make sure your vendor reviews are performed by qualified subject matter experts vs casual subject matter enthusiasts.



17

Never sign a contract before due diligence has been completed.

Due diligence is the process of identifying and evaluating a vendor's risk practices and controls. It's not unusual to discover process gaps, insufficient controls, or other issues during vendor due diligence. In these cases where risk and issue mitigation are required, your organization should make every effort to ensure the mitigation is satisfactory before signing the contract.

Once you've executed the contract, you've reduced your leverage to make the vendor correct any issues. And while the best vendors will show good faith efforts to work with their clients to correct issues, many vendors only abide by what is in the contract. If they're not legally obliged to fix the problem, they won't. This is especially true when the issue mitigation may be costly or require additional vendor resources, so make sure due diligence is complete and any identified issues are corrected before executing the contract.

If issue mitigation is acceptable post-contract execution, make sure you include those details in your agreement. Ensure the contract identifies specific remediation requirements, evidence of correction, and the timing for closing the issue.

18

Identify standard required contract terms and conditions for your high-risk and critical contracts.

Contracts are one of your best third-party risk management tools, but they can only be effective when structured to protect your organization and its customers. The best way to ensure contracts are well written and can mitigate risks to the organization is to create a standardized set of terms and conditions to include in every high-risk and critical contract. These should include indemnification and insurance, a right to audit clause, service level agreements, regulatory compliance, handling customer and consumer complaints, cybersecurity and privacy protection, business continuity and disaster recovery planning, breach notification requirements, and more.

It's also important to track and manage exceptions where the standard terms and conditions are not included in a contract. Either because it's an existing contract, you have no leverage because the contract is a non-negotiable terms of service agreement, or because they were negotiated out. Keeping track of this information will help you understand where you may have additional contract risk and prepare you for future amendments or negotiations.

19

Conduct a full contract review at the midpoint of the contract term.

Unfortunately, it's not uncommon for organizations to lose track of contract expiration dates only to realize a renewal is just days away. Because of the lack of preparation, there's little to no time to negotiate better terms or identify alternative vendors that can provide more value to your organization or customers. This frequently results in unfavorable contract renewals.

A full contract review is recommended at the midpoint of the contract term to avoid this situation. At the halfway point of the contract, your organization should be able to determine if there's a need to renegotiate the contract, adjust service level agreements, or request changes in pricing, delivery, etc. This approach will give you ample time to prepare for renegotiation or conduct RFPs for alternative vendors.

Remember, the more complex the product or service, the longer the negotiations will take. It can also take a lot of time to identify and vet alternatives, so give your organization time to plan ahead if you want to explore other vendor options rather than renewing with your existing one.

20

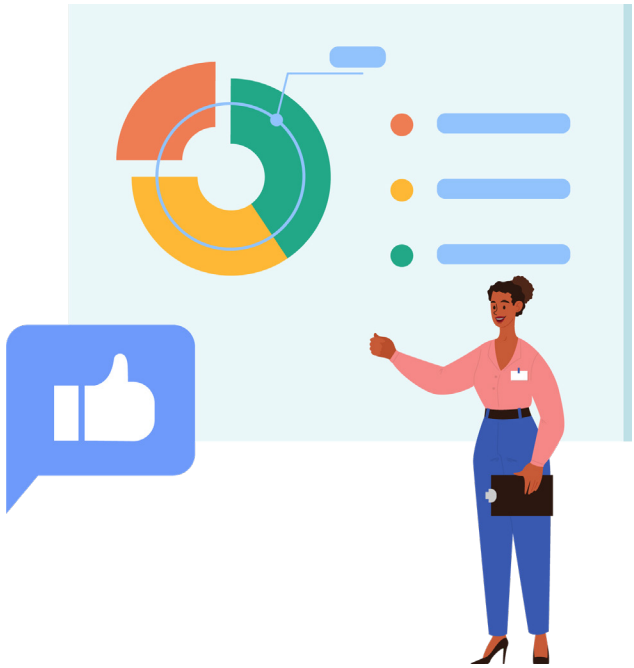
Track and manage vendor performance.

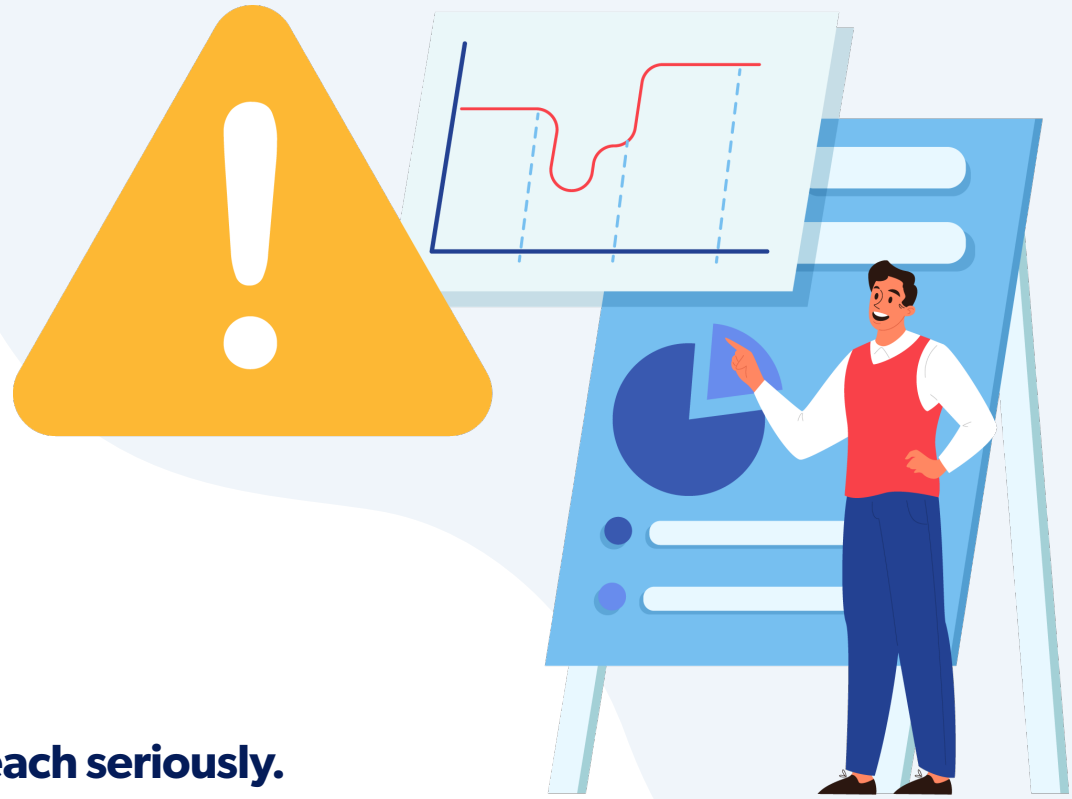
Third-party risk management includes managing the risk of poor vendor performance. Your organization cannot realize a vendor relationship's full and intended value if it's not performing at the expected level. Additionally, declining performance can often indicate the presence of other risks that need to be investigated.

Your vendor's performance matters every day, so it's important to define your performance expectations and then monitor them closely. Remember that performance management makes it much easier to identify and correct small performance issues before they become big problems for the organization.

EXAMPLE

Suppose your customer service vendor shows decreased satisfaction scores and longer hold times. This may be because there have been reductions in staff due to the vendor's degrading finances, or maybe the vendor's product quality is dramatically lower than usual, and they may have unmanaged supply chain risks.





21

Take every breach seriously.

The infamous MOVEit data breach of 2023 brought much-needed awareness to third-party cybersecurity risk. Many organizations that were impacted in this breach didn't use MOVEit themselves, but instead were partnering with third parties that used the software. Third-party cybersecurity attacks and data breaches are painfully commonplace these days. And as they say, it's not a matter of if your organization will be affected; it's a matter of when. As a result, all breaches and cybersecurity incidents deserve serious attention. Suppose your vendor has suffered a data breach but has assured you that your data wasn't affected. In this case, you may be tempted to take a more casual attitude of, "it doesn't affect us, so it doesn't matter." This perspective is not only misguided, but it's also dangerous.

Remember that whenever your vendor suffers a cybersecurity attack or data breach, you must respond as if it affects your organization every time because, ultimately, it does. Whenever there has been a cyber breach, you must be sure how they determined if your data was affected or not, the cause of the breach, and the remediation attempts in process to prevent another occurrence. Moving forward, you must closely monitor your vendor's cybersecurity risk profile. Don't be afraid to do ad-hoc due diligence and vendor risk reviews with your SMEs to ensure your organization is well protected.

22

Monitor vendor financial health.

As the economy fluctuates and faces new challenges with supply chain issues, bank failures, and global events, it's important to stay on top of your vendor's financial health. Sudden declines in your vendor's finances can lead to declining service levels, reputational damage, and an inability to deliver products and services your organization relies on. Watch for signs of declining financial performance, such as layoffs and staff reductions, bad press and litigation, and merger and acquisition activities.

Be sure to also request your vendor's financial statements periodically, like the income statement, balance sheet, and cash flow statement. These three documents can reveal the state of your vendor's finances and long-term viability.

23

Consider vendor risk monitoring and alert services.

Day-to-day monitoring of vendor risk can be challenging. Typically, it involves setting up internet search alerts for your vendor or your vendor's industry. While you may occasionally get a good piece of information, it takes a lot of time and attention, and many alerts aren't timely or particularly relevant.

The good news is that nowadays many professional services organizations specialize in monitoring vendor risk. Often, these services are subscription based, allowing you to monitor a few or many of your vendors. These services usually specialize in one or more risk domains. They can help monitor your vendor's cybersecurity posture, finances and credit, regulatory compliance, reputation, and environmental, social, and governance risks.

By using these services, your organization will have access to more relevant information sooner, allowing it to take immediate action when necessary.

24

Make sure your risk assessment tools reflect the current risk environment.

Third-party risk management requires a good risk identification methodology and tools. Your inherent risk assessment, vendor risk questionnaire, and due diligence document requirements should always reflect the current risk environment. Work with your SMEs once a year to review (and update as needed) your risk assessments, vendor questionnaires, and standards for due diligence documentation. This will ensure your tools are current and can effectively address any new or emerging risks.

25

Engage the board and senior management.

The success of any third-party risk management program largely depends on the tone-from-the-top, meaning the board and senior management considers third-party risk management a priority and integrates it into the organization's strategy and business decisions. It also means they're regularly engaged in third-party risk management through reporting, updates, and approval of the third-party risk management policy. This engagement is not only a best practice, but a regulatory expectation for many organizations.

Suppose your board and senior management aren't engaged with third-party risk management. In that case, you must work with your management to identify ways to increase their involvement. For many regulated industries, it may be as simple as referencing the regulatory guidance that details the board and senior management's roles and responsibilities for third-party risk management.

venminder

26

Collaborate with and solicit feedback from your stakeholders.

Third-party risk management is a "team sport" requiring the skills and participation of different stakeholders. Collaborating with your stakeholders, from vendor owners to SMEs to other risk management teams, will ensure a more balanced and effective third-party risk management program. Make sure you communicate with your stakeholders regularly regarding new or changing requirements and solicit their feedback before implementing major changes. Communication and collaboration will pave the way for long-term third-party risk management success.

27

Develop and implement third-party risk management program metrics.

Can you articulate the health, stability, and effectiveness of your third-party risk management program? Using third-party risk management program metrics can help your board and management think beyond regulatory compliance and gain a deeper understanding of the effectiveness of your third-party risk management program and how risk is managed across your vendor portfolio. Program metrics might include the number of due diligence reviews that result in vendor approvals vs denials or the percentage of vendors that are meeting your performance standards.

Data-driven metrics can also help management make decisions and drive action. The right metrics can help your management understand where there is a need for a bigger budget or additional resources or if internal compliance is a real issue.

28

Use third-party risk management software.

Manual processes are not just inefficient and time-consuming; they are also extremely error-prone. When it comes to third-party risk management, technology is your friend. Using software specifically designed to address the many complex and interrelated processes involved in third-party risk management can help you standardize and automate your workflows, manage document collection and storage, communicate more effectively with your vendors and internal stakeholders, generate reporting, and maximize your limited resources. In many cases, specialized third-party risk management software can help you accomplish more without the additional cost of full-time employees (FTEs).

29

Consider outsourcing to optimize existing resources.

Third-party risk management programs are notorious for being lean, particularly during times of economic hardship. But even the most experienced and effective third-party risk management practitioner can only accomplish so much in a single day. It doesn't take much extra work to create a permanent backlog and build a domino effect of long wait times to get vendors up and running.

If your third-party risk management team is at maximum full capacity but still has too much work, consider outsourcing certain aspects of your third-party risk management process to a qualified third-party risk management services provider. You can find services ranging from due diligence document collection to contract management to supplying qualified SMEs to perform vendor risk assessments. Outsourcing low-value but high-effort processes, like due diligence document collection, can give your team more bandwidth to identify and manage risk.

30

Join a third-party risk management peer group or professional organization.

In some ways, third-party risk management can feel like a niche practice, especially when it's not widely understood in your organization. In these situations, it can be difficult to get advice or support when you have questions about third-party risk management. Even for seasoned third-party risk management professionals, there are times when you just need to connect with others that understand your role and its challenges and can offer practical advice.

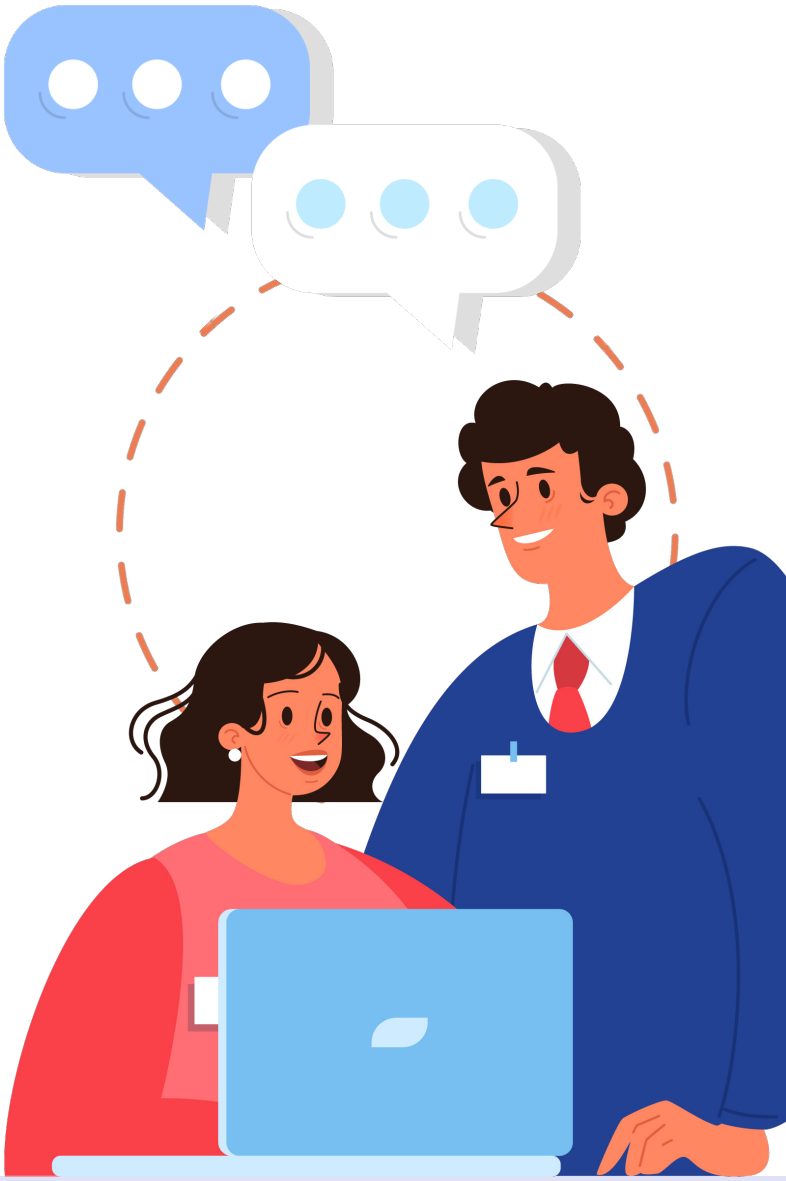
Peer groups and professional organizations can be a great way to network, share best practices, gain new perspectives, and increase your third-party risk management knowledge. Whether posting a question to an online forum or attending a third-party risk management conference, staying in touch with the third-party risk management community has many benefits.

31

Never stop learning about new and emerging risks.

Geopolitical risks from ongoing wars, environmental, social, and governance (ESG) concerns, economic instability, and artificial intelligence (AI) continue to make headlines in the world of third-party risk management. The risk landscape is constantly changing, and third-party risk management practitioners must keep pace with all the new and emerging risks, including regulatory updates and changes. Make sure you dedicate time to keep learning, whether through a formal training program or attending online webinars and workshops. Sign up for industry and regulator news alerts, research new risk topics, and talk to your third-party risk management peers in your industry and other industries.

New and emerging risks are always on the radar of successful third-party risk management practitioners, who develop best practices for managing them. As a third-party risk management professional, you must be committed to continuous improvement for your program and your professional growth and development.



And there they are! A well-rounded list of 31 third-party risk management best practices for 2024 and beyond. Of course, this list shouldn't be considered all-inclusive, but it can get you started on the right path to improving your current third-party risk management practices.

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.