LexisNexis®

Nexis® Solutions

Third-Party Risk Management

What is third-party risk management?

Third-party risk management (TPRM) meaning – The process of identifying and managing the risks associated with outsourcing tasks to third-party vendors or suppliers. The aim is to ensure that a company's operations, reputation, and sensitive information are protected from potential risks and breaches caused by third-party vendors. The TPRM process includes several stages such as identifying whether you need to employ a third party, conducting due diligence, shortlisting and selection, sending a risk questionnaire, drafting a contract, beginning the onboarding process, implementing ongoing monitoring, undertaking internal audits, and contract termination or offboarding. These TPRM lifecycle stages help organizations manage third-party risk and ensure that their vendors meet the same standards and expectations for cybersecurity and data privacy as their internal teams.

TPRM LIFECYCLE & ITS STAGES:

What is a third-party risk management lifecycle? The TPRM lifecycle is an ongoing process that requires ongoing attention and regular reassessment to ensure that risks are being appropriately managed. The stages involved in the TPRM lifecycle are:

1 Planning and scoping

This stage involves identifying the third-party relationships that need to be assessed and defining the scope of the assessment. It is essential to understand the business processes that are supported by the third-party relationship, the criticality of those processes to the organization, and the potential impact of any disruption. Before hiring a third party, creating a checklist of criteria can help you make more informed decisions. Some additional points that can be included on your checklist:

- Evaluating the cost of hiring a third party.
- Assessing the reputation and reliability of the third party. Check reviews, testimonials, and references to ensure they have a track record of delivering quality work.
- Determine the scope of work and the level of involvement required from the third party.
- Consider the potential risks associated with hiring a third party, such as data breaches, intellectual property theft, or reputational damage.
- Clarify the deliverables and deadlines with the third party.
- Discuss the communication channels and reporting mechanisms with the third party.
- Ensure that the third party complies with relevant regulations and standards, such as data protection laws or industry-specific regulations.

By carefully evaluating these factors and weighing the benefits against the risks, you can make an informed decision to hire a third party and choose the right partner for your needs.

2 Due diligence and third-party selection

This stage involves collecting information about potential third-party vendors and evaluating them against predetermined criteria. Due diligence may involve reviewing financial statements, legal documents, and security controls, among other things. It's important to have a robust selection process for third-party suppliers. Some steps to take for third-party due diligence:

- Develop clear criteria for shortlisting: Determining the key factors such as vendor experience, financial stability, technical capabilities, and regulatory compliance, that are important for your organization and using these criteria to create a shortlist of vendors that meet your requirements.
- Assess vendor risk: Conduct a risk assessment of each shortlisted vendor. Consider the vendor's location, security posture, financial stability, and regulatory compliance and use this information to create a risk profile for each vendor.
- Evaluate vendor performance: Gather information on each vendor's performance from their current or previous customers. This can help you know how well they deliver on their promises, how responsive they are to issues, and how well they communicate.
- Conduct due diligence on each vendor. Consider the vendor's business integrity and ESG standards, as well as any certifications they hold.
- Shortlist presentation: When presenting the shortlist to decision-makers, be transparent about the reasons each vendor has been shortlisted and any risk factors they should be aware of. Provide a full and fair view of the risks posed by each appointment.

3 Tailoring Risk Questionnaire to selected third parties

When tailoring your Third-Party Risk Management (TPRM) questionnaire, it's essential to consider the specific needs and requirements of your organization and the third-party providers you are evaluating. Here are some factors to keep in mind:

- Risk profile: Different third-party providers may pose different levels of risk to your organization. For example, a provider with access to your company's confidential data may pose a higher risk than a provider that only provides basic services. Consider tailoring your questionnaire to ask more detailed questions of higher-risk providers.
- Considering Industry-specific regulatory or compliance requirements & ensure that your third-party providers are meeting the necessary standards.
- Contractual obligations: Your organization may have specific contractual obligations that your third-party providers must meet. Ensure that your questionnaire gathers the necessary information to evaluate these obligations.
- Existing relationships: If you already have an existing relationship with a third-party provider, your questionnaire may need to gather additional information about changes to their risk profile or compliance posture since your last evaluation.
- Geographic location: Consider tailoring your questionnaire to gather information about any additional risks associated with operating in specific countries or regions.
- Emerging risks: Regularly review and update your questionnaire to ensure that it is addressing the latest risks and threats.
- Remember, the goal of your TPRM questionnaire is to gather the necessary information to evaluate the risk posed by third-party providers and ensure that they are meeting your organization's requirements. By tailoring your questionnaire to the specific needs of your organization, you can better evaluate third-party risk and make more informed decisions about supplier selection.

4 Contract negotiation

Once a vendor has been selected, the organization must negotiate a contract that includes appropriate terms and conditions to protect the organization's interests. This includes defining roles and responsibilities, service level agreements, and security requirements.

5 Vendor/Supplier Ongoing Process

When it comes to onboarding suppliers, it's important to take a comprehensive approach that addresses not only the initial introduction and orientation but also the ongoing management of the relationship. Here are some key steps that can be considered when formalizing your supplier onboarding process:

- Collecting relevant supplier information their contact details, product or service offerings, and any certifications or qualifications they may have.
- Perform due diligence or thorough assessment of the supplier's capabilities, financial stability, and compliance with regulations and industry standards.
- Outlining contractual terms and conditions with the supplier, including pricing, delivery timelines, and quality expectations.
- Develop an onboarding plan that outlines the steps and timelines for integrating the supplier into your organization. This should include any necessary training, system access, and other requirements.
- Regularly assess the supplier's performance and compliance with contractual terms, and address any issues that arise in a timely manner.

By following these steps, you can establish a robust and effective supplier onboarding process that helps ensure the success of your relationship with your suppliers.

6 Ongoing monitoring and oversight

Implementing ongoing monitoring in third-party risk management requires a structured approach that involves regular assessments and reviews of your third-party vendors. Some steps to implement ongoing monitoring are:

- Define the monitoring strategy including the scope of the monitoring activities, the frequency of assessments, and the key risk indicators (KRIs) and key performance indicators (KPIs) you will use to measure vendor performance and risk. This strategy should be tailored to the specific risks and requirements of your organization.
- Conduct regular third-party vendor's risk assessments to identify potential risks and evaluate the effectiveness of their risk management controls. This can involve reviewing their security controls, compliance practices, financial stability, and other relevant factors.
- Monitor vendor compliance with relevant regulations, standards, and contractual requirements. This can involve reviewing compliance reports, conducting audits or assessments, and requesting evidence of compliance.
- Track vendor performance against agreed-upon SLAs and performance requirements. This can involve reviewing performance reports, conducting surveys or feedback sessions, and analyzing other relevant data.
- Review your contracts with third-party vendors on a regular basis to ensure that they remain up to date and reflect any changes in the relationship or the risks involved.
- Establish a feedback loop with your third-party vendors to ensure that they are aware of your monitoring activities and any issues that arise. This can help facilitate open communication and improve the effectiveness of your ongoing monitoring efforts.

By implementing ongoing monitoring in third-party risk management, you can help ensure that your organization is well protected against potential risks and that your relationships with your vendors remain productive and beneficial over the long term.

7 Undertake Internal audit

Involving your internal audit team in third-party risk management can be highly beneficial for your organization. Here are some ways in which your internal audit team can contribute to third-party risk management:

- Independent review: Your internal audit team can provide an independent review of your third-party risk management program, including your monitoring activities, risk assessments, and vendor due diligence processes. This can help identify any gaps or weaknesses in your program and provide recommendations for improvement.
- Consistency and automation: Your internal audit team may have established methods for assessing and reporting on third-party risks, which can bring consistency and potentially automate certain aspects of the process. This can improve efficiency and effectiveness in third-party risk management.
- Specialized expertise: Internal auditors often have specialized expertise in risk management, compliance, and other relevant areas. This can be particularly valuable in assessing third-party risks and identifying ways to mitigate those risks.
- Reporting and communication: Your internal audit team can help improve reporting and communication around third-party risks, providing regular updates to senior management and the board of directors. This can help ensure that key stakeholders are informed about the risks and the effectiveness of your risk management program.

Overall, involving your internal audit team in third-party risk management can help enhance the effectiveness and efficiency of your program, while providing an extra layer of rigor and independent review.

8 Termination and offboarding

Contract termination and "offboarding" are important steps in the third-party risk management lifecycle. They involve the process of ending a contractual relationship with a vendor or supplier, whether planned or unplanned, while minimizing any potential risks to your organization. Here are some key considerations when terminating a contract with a vendor or supplier:

- Revoking access: The first step in offboarding a vendor or supplier is to revoke their access to your systems, premises, and data. This can include disabling user accounts, removing physical access badges or keys, and restricting access to your network and data.
- Documenting reasons: It is important to document the reasons for the contract termination, whether they are planned or unplanned. This documentation can help mitigate any potential legal or reputational risks that may arise from the termination.
- Reviewing contract terms: Review the contract terms and any associated SLAs and KPIs to ensure that all obligations have been fulfilled by the supplier. This can include verifying that all deliverables have been completed, all payments have been made, and all data and property have been returned to your organization.
- Notifying stakeholders: Inform all stakeholders, including senior management and any internal teams that may be affected by the contract termination. This can help ensure that everyone is aware of the situation and can take appropriate actions to mitigate any risks.
- Conduct exit interviews: If appropriate, conduct exit interviews with the vendor or supplier to gather feedback on their experience working with your organization. This can provide valuable insights into potential areas for improvement in your third-party risk management program.

By following these steps, you can help ensure that the contract termination and offboarding process is completed in a structured and controlled manner, minimizing any potential risks to your organization.

For more information:

Email us at information@lexisnexis.com

LexisNexis®