



Best Practices in End-to-End Third- Party Risk Management

Introduction

End-to-end third-party risk management refers to identifying, assessing, mitigating, and monitoring risks associated with third-party vendors, suppliers, distributors, sales agents, and other partners. It involves evaluating the potential risks arising from your organization's relationship with a third party – such as risks of bribery and corruption, fraud, sanctions violations, conflicts of interest, kickbacks, data breaches, human rights violations, and overall financial and operational viability – and implementing measures to reduce or mitigate those risks.

This process typically involves conducting due diligence on potential third parties, establishing contractual agreements that outline expectations and requirements and monitoring them. Effective end-to-end third-party risk management requires a comprehensive and integrated approach that involves collaboration across departments and functions within an organization at all stages of the third-party relationship.

End-to-end third-party risk management is critical for any organization that relies on third parties to deliver goods and services or to assist in making sales. It involves a comprehensive approach to identifying, assessing, and mitigating the risks associated with these third-party relationships.

For Chief Compliance Officers, third-party risk management is especially important as it can help ensure their organizations remain compliant with relevant laws, regulations, and standards. Compliance officers are responsible for managing risk across all areas of the organization, and third-party relationships are often central to the risk in those areas. Failure to effectively manage these risks can result in legal and financial consequences and damage to an organization's reputation and enterprise value.

Despite its importance, third-party risk management can be challenging for compliance officers. The complexity and diversity of third-party relationships, coupled with the rapid pace of change in today's business and geopolitical environment, can make it challenging to keep up with the evolving risks associated with these relationships.

Furthermore, compliance officers often have limited resources and must prioritize their efforts to manage the most critical risks.

In this white paper, we will explore the key challenges of third-party risk management and provide practical guidance on how compliance officers can effectively manage these risks. We will discuss each stage of the third-party risk management process, from needs assessment to scoring and due diligence, approval, contracting and mitigation, ongoing monitoring, and renewal or offboarding, and provide relevant resources to support our recommendations. By following the guidance in this white paper, compliance officers can ensure that their organizations are effectively managing third-party risks and are well-positioned to meet their compliance obligations.



Needs Assessment

During the needs assessment stage, an organization evaluates its business needs and determines whether a third party is required to fulfill them. The organization should identify the specific requirements and criteria for the third party, such as compliance program requirements, relevant expertise and staffing, quality standards, and security requirements. The organization then should assess whether an existing third party can fulfill the need or whether a new third-party engagement is warranted.

Validate Need

The third-party process should begin with validation that a third-party relationship is, in fact, necessary. In some cases, internal company personnel may be better equipped to manage the business need, given their pre-existing expertise of the company and its business. In other cases, such as sales activities, using internal company personnel may involve less risk than hiring a third party, and a risk-based decision might be made not to pursue a third-party engagement. This stage of the process may involve broader market intelligence gathering on third-party capabilities, such as reviewing third-party documentation, conducting interviews with third parties, seeking referrals from fellow employees, industry peers, or experts, or issuing requests for information (RFIs).

Define Business Rationale

After validating the need for a third party, the organization should clearly define the business rationale for engaging with a third party. The rationale should establish the third-party relationship's goals and objectives, define the scope of work or services to be provided by the vendor, and identify the benefits and risks associated with the relationship. The business rationale process should also begin to contemplate the third party's eventual legal, regulatory, and contractual requirements.

Search Existing Parties

Once the need and business rationale have been established, a business sponsor within the organization should be identified to own the accountability for onboarding the third party. That business sponsor should always begin with a search for third parties the organization already uses that can meet its identified needs. The process may involve researching existing third parties, seeking referrals from fellow employees, industry peers, or experts, or issuing requests for proposals (RFPs) or RFIs to existing third parties. A proper search that ensures that no other existing third party can satisfy the need can ensure that an organization's third-party base does not grow unnecessarily, as each new third party increases the risk exposure of the organization. In some scenarios, an existing third party's work may need to be expanded, in which case the organization should provide a process by which a new engagement for an existing third party can be initiated.

Complete Rationale Documentation

Once the business need has been established, and the business sponsor has established that a new third party, or a new engagement with an existing third party, is required, the organization should have a formal documentation process whereby the business sponsor must provide written details about the business need as well as information the business sponsor already knows about the third party, such as its qualifications and how they relate to the business need, where it will operate and what type of work it will do, whether it has connections with government officials or other known risk factors and whether it will handle sensitive organization or customer information. Ideally, the organization should have some form of technology to manage this business rationale documentation to ensure the organization has a clear repository of this critical information, with an audit trail, and to ensure that the following steps in the diligence process outlined below can be more easily managed and monitored in that technology. Managing these steps over email or over simple shared drives or basic form systems not designed for third-party due diligence can create gaps and challenges for business users, particularly as the end-to-end process scales within the organization.

Scoring and Due-Diligence

In this stage, the organization scores and evaluates potential third-party engagements based on specific criteria and risk areas defined by the organization, such as ethics and compliance risk, financial and operational stability, information security, sanctions exposure, and overall reputation. This stage may also involve requesting due diligence questionnaires from the third party to assess its capabilities, track record, and potential risks and conducting more in-depth enhanced due diligence on the third party using external providers.

Calculate Profile Risk Score

After the business sponsor completes its business rationale documentation and provides baseline information about the organization, the organization should calculate an initial profile risk score for the third-party engagement. If the engagement is a new engagement for an existing third party, it should be scored separately, as the new scope of work might be higher or lower risk than the initial scope of work for the third party.

The profile score can be based on various responses from the initial documentation, which can be weighted as percentages or be assigned specific absolute values. If the organization views risk across multiple risk areas (e.g., ethics and compliance, information security, human rights), then the engagement should have separate risk scoring for each risk area. These scores are usually mapped to some risk level, such as Low, Medium, High, Very High, etc.

Again, a technology platform should ideally automate this process, as manual or spreadsheet-based approaches are prone to error, are not user- friendly, and are difficult to monitor and audit.

Automate Review and Approval

Once the third parties have been initially scored and assigned a risk level, the organization can automate the review and approval process using software or other tools to ensure consistency and efficiency in the decision-making process. An intelligent technology might even offer to automatically record completed diligence on an engagement that is very low risk without any human review. Higher risk-scored third parties may require additional levels of approval as well as additional due diligence steps, such as enhanced due diligence.

Deploy Appropriate Due Diligence Questionnaires

In this stage, the organization should deploy appropriate due diligence questionnaires to the selected third party to gather more detailed information about their business practices, security measures, compliance with regulations, and other relevant factors that may impact the relationship. If the organization covers multiple risk areas, it might consider sending separate specific questionnaires rather than one large questionnaire so that during the review process, only certain questionnaires can be sent back to the third party for editing. Responses from the due diligence questionnaires may increase the risk score and level for specific risk areas if the third party provides information indicative of risk that was unknown during the business sponsor rationale documentation process. A technology can manage this process seamlessly while maintaining a thorough audit trail for each version of the questionnaire.

Complete Watchlist Screening

The organization should also conduct watchlist screening to ensure that the proposed third parties and individuals affiliated with them are not on any government sanctions or other watchlists, not related to politically exposed persons (PEPs), and do not have other adverse media that might increase their risk.

Conduct Enhanced Due Diligence

Finally, for third parties with higher risk scores, the organization should conduct enhanced due diligence, which involves a more in-depth investigation of the third party by independent expert services firms. Enhanced due diligence may include site visits, interviews with key personnel and other sources in the industry, and additional research and analysis to ensure that engaging the third party would not pose serious risks to the organization. A technology can usually manage ordering and tracking these reports more seamlessly than manually over email.

Adjust Risk Scores and Levels

After the initial profile score is calculated, the additional due diligence steps described above (e.g., enhanced due diligence, watchlist screening, etc.) may produce additional information indicative of risk that was previously unknown. The third-party process should allow permissioned users to be able to further increase the third party's engagement risk score within each risk area based on this new information. For example, a third party might be medium risk from a bribery and corruption perspective based on the responses provided in the business rationale and due diligence questionnaire, but their score and level may be adjusted to higher risk based on information an enhanced due diligence provider discovers during its interviews with customers of the third party. Similarly, the engagement risk scores by risk area should also be adjustable downwards, based on mitigation items (discussed below), which reduce the overall risk exposure. Ultimately, this should result in the engagement having a final risk score and level per risk area, which ultimately will drive the final set of approvers for the engagement.

Approval, Contracting & Mitigation

In this stage, the organization approves the selected third party, negotiates contractual terms and conditions, and executes risk mitigation measures to manage and reduce the risks associated with the third-party relationship. Again, a technology-driven approach is essential for managing all of these steps most effectively.

Define Appropriate Risk Mitigations

The organization should define appropriate risk mitigation measures based on the third party's risk profile and the identified risks associated with the relationship. These risk mitigations could include establishing payment monitoring, site visits, and other audits, new security controls, performance monitoring, or additional insurance coverage.

Complete Risk-Based Approvals

In this stage, the organization should complete risk-based approvals for the selected third parties based on their ultimate risk scores. These approvals should be documented and maintained for future reference.

Complete Contracting & Mitigations

After the organization completes its risk-based approvals, it should finalize and execute the contract with the selected third party. The contract should include the agreed-upon terms, conditions, and risk mitigation measures, and those mitigations can continue to be executed, such as providing training to the third party.

Connect with ERP/Vendor Creation Process

Finally, the organization should connect the third-party risk management process with the enterprise resource planning (ERP) system to ensure that the approved third parties are adequately onboarded and integrated into the organization's systems and processes.

Ongoing Monitoring & Renewal or Offboarding

In this stage, the organization continuously monitors the selected third parties, renews the third-party engagement as needed, or offboards the engagement or overall third party when the relationship is no longer necessary or poses too much risk.

Automate Ongoing Watchlist Screening

The organization should automate ongoing watchlist screening to ensure that no new problematic information about the selected third party is publicly available after it is engaged. This ongoing monitoring typically runs daily and should be seamlessly integrated into the end-to-end risk management process. New information might lead to termination of the engagement or the third party or new mitigation measures.

Automate Transaction-Level Compliance Monitoring

The organization should also automate transaction-level compliance monitoring to detect any unusual or suspicious activity that may indicate a higher risk of non-compliance. With regard to financial integrity risks, such as bribery, fraud, embezzlement, sanctions, and conflicts of interest, compliance monitoring for vendors should involve automated extraction of payment data, consolidating purchase requisition, purchase order, invoice, and payment data, and applying advanced forensic analyses to all of that data to risk score the overall transaction.

For sales intermediaries, such as distributors, it would involve similar analyses on the customer revenue transactions of the organization to look for unusual patterns of discounts, rebates, free goods, and the like. Transaction-level monitoring ensures that third parties that may look sound during the diligence process but behave in an untoward way once engaged are flagged immediately, and remedial action is taken by the compliance team. For other risks, such as cybersecurity risks, security monitoring platforms exist that perform ongoing testing of third parties.

Notably, when an organization is setting up a third-party management program for a universe of thousands of existing third parties, beginning the process with transaction-level compliance monitoring can be a powerful way to immediately monitor third parties for non-compliance while the due diligence process is stood up. The data from the compliance monitoring program, which can aggregate transaction risk scores for each third party to provide an average risk score for the third party itself, can then be used to determine the organization's highest-risk third parties. This determination will be far more objective and data-driven than more informal approaches, such as surveying employees in each market to identify the highest-risk third parties.

Perform Performance Reviews & Audits

The organization should conduct periodic performance reviews and audits of its highest-risk third parties to assess their compliance with contractual terms, ethical requirements, and regulatory requirements. These reviews should be documented and maintained for future reference.

Renew Due Diligence on a Risk-Basis or Offboard

Based on the results of the ongoing monitoring, the organization should renew due diligence on a risk basis for third-party engagements or offboard those engagements, or the third parties themselves, that are no longer needed or do not meet the organization's risk management standards. Renewing due diligence on a risk basis involves conducting additional due diligence procedures to ensure that the third party continues to meet the organization's risk management criteria, typically including refreshing the steps described above. Offboarding engagements or third parties involves terminating the contract or overall relationship and transferring any relevant data or services to another third party or internal resources.

Overall, the ongoing monitoring, renewal, and offboarding stages are critical for maintaining an effective third-party risk management program. By continuously monitoring the selected third parties, the organization can detect and respond to potential risks in a timely manner, renew the relationship as needed, and offboard third parties that no longer meet the organization's risk management standards.

Conclusion

In summary, end-to-end third-party risk management is a comprehensive process that enables organizations to identify, assess, and mitigate risks associated with their relationships with vendors, suppliers, distributors, sales agents, and other partners. The process involves several stages, including needs assessment, scoring and due diligence, approval, contracting, and mitigation, ongoing monitoring, and renewal or offboarding. Each stage of the process is designed to ensure that the organization selects and manages third-party relationships in a way that minimizes the risks associated with those relationships. By implementing an end-to-end third-party risk management program, organizations can improve their risk posture, protect their data and assets, maintain compliance with regulatory requirements, and ultimately protect their reputation and enterprise value.


One-on-One Advice


Our team of experts has implemented Case IQ for compliance teams around the world.

They are available - free of charge - to speak with you and share the best practices we've learned. No pushy salespeople, just a chance for you to learn from our experts.

With our suite of compliance tools, reporting hotline, and case management software, plus a 25-year track record of successful implementations, Case IQ is the global leader for end-to-end compliance risk management. To get a demo please visit www.caseiq.com/request-a-demo.

To book your one-on-one, please contact:

 (800) 465-6089

 sales@caseiq.com
media@caseiq.com
support@caseiq.com

 300 March Road
Suite 501 Ottawa,
Ontario K2K 2E2
Canada



DON'T MISS OUT

Visit CaseIQ.com for more great investigation resources.