5 Best Practices to Enhance Third-party Due Diligence
Introduction

Outsourcing has become a necessity to save on costs and labor, to free up infrastructure, to compete at local and international levels and concentrate on core business activities. However, outsourcing comes with its own share of multiple risks such as IT, corruption, operations, business continuity, and regulatory compliance.

Most organizations assess these risks when finalizing a third-party. However, third-party management and due-diligence usually take a back seat after the third-party has been brought onboard. This makes organizations unaware of likely third-party risks, which, if left unmitigated can snowball into critical issues that could significantly affect the profitability and reputation of the organization. It doesn’t matter if the fault is on the third-party’s side. Ultimately, the company that hired the third-party is held responsible by regulators and customers for not identifying and addressing the issue.

Staying competitive requires organizations to not only expand their third-party network but also validate the sustainability of their third-party network. Conducting business with a high-risk or non-compliant third-party can significantly tarnish an organization's reputation and lead to heavy fines, penalties, and costly product recalls.

Multiple regulations such as - Health Insurance Portability and Accountability Act (HIPAA), Anti-Money Laundering (AML) requirements, Conflict Minerals Reporting requirements, the Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, the Federal Trade Commission (FTC) Act, Office of the Comptroller of the Currency (OCC), and the Dodd-Frank Act have increased the focus on third-party governance. Thus, organizations need to be doubly sure of the third-party they take onboard as well and of those that they continue to have a relationship with.

As organizations benefit from outsourcing, they also face the challenges of managing the vast network of third-party spread across geographies. With limited resources, it becomes extremely difficult to ensure focus on third-party performance management, third-party risk, and compliance monitoring. Additionally, a vast amount of third-party information including contact, financial and business information, contracts, agreements, certifications, risk assessments, compliance assessments, and audit results become unmanageable. As such, organizations adopt ad-hoc processes to monitor third-party and ensure regulatory compliance, which often do not highlight the critical issues and thus limits the organization's ability to respond to eventualities.

Steps to Strengthen Third-Party Due Diligence

Trust is an integral part of building third-party relationship, however that's not enough. Companies and their branches spread across the world often straddle with the same third-party unaware of risks it can cause. Companies must be aware of the risks that the relationship with third-party can cause. They need to improve visibility of the supply chain and also improve vigilance.

1. **Assimilate and centralize third-party information**

   Large third-party base often leads to important information getting lost as there is a lack of visibility. As a result, most organizations often do not even know of other business units that work with the same third-party. Therefore, it is important to have a consolidated third-party information system and keep third-party in check. Information including, business details, financial status, certifications, contracts, location, associated business units, roles and responsibilities will help with searching third-party agreements, assessment results, background checks and other details.

   Centralized third-party information improves the accessibility of information globally, as well as details about negotiations and risk mitigation activities.

2. **Onboard and screen third-party based on business relationship**

   Most organizations screen third-party at the time of onboarding, and it remains a crucial step before entering into a contract. Therefore, the screening process needs to be well-defined and automated, and should provide input on the criticality of the third-party relationship. Information including the type of business, accessibility of the third-party to sensitive information, dependency, business continuity, spend and financial and legal are important factors on which a third-party needs to be
Gain valuable intelligence and visibility into third-party relationships for risk awareness and informed business decisions. Centralize the inventory of third-party information for enhanced management of third-party screening, onboarding, risk, compliance, audits and issue management processes. Effective due-diligence requires an in-depth understanding of third-party. Organizations need to know their risk appetite and continuously assess risks brought in by their third-party. Based on this information, they need to define the progress of the relationship.

In order to deploy a resilient third-party due-diligence program, organizations need a transparent system which can enable them to know their third-party base, segment them, quickly assess their sub-third-party, deploy controls, and respond quickly to issues. A robust technology will not only automate this process, but also empower organizations with consolidated reports for improved decision making.

Organizations can leverage third-party management programs to:

- Gain valuable intelligence and visibility into third-party relationships for risk awareness and informed business decisions
- Centralize the inventory of third-party information for enhanced management of third-party screening, onboarding, risk, compliance, audits and issue management processes
- Seamlessly collaborate internally and with third-party to ensure that the due-diligence redundancies are curtailed and the costs are optimized
- Establish consistent, appropriate and proportionate due-diligence based on the type of third-party and the context of that relationship
- Focus due-diligence efforts on critical third-party by automating risk-based segmentation and deploying rules for continuous due-diligence
- Validate third-party with rich, real-time, global data feeds covering: Politically Exposed Persons including relatives and close associates, Sanctions listings (U.N., OFAC and others), Special Interest Persons, Stated Owned Enterprises and board members lists, and adverse media.

3 Define a process for ongoing third-party monitoring

As the number of third-party in an organization increase over time, one of the best strategies is to conduct due-diligence based on the associated risk tiers. The risk tiers can be derived by stratifying third-party based on the segmentation score or the risk profile. This process helps streamline the efforts made in conducting due-diligence across the third-party base. By defining specific rules or criteria for each type of third-party, organizations can reduce the burden of due-diligence and also ensure that strategic third-party are tracked better.

As this task can be resource intensive, organizations should automate the process and base it on well-defined algorithms for scheduling third-party monitoring activities. This regular input of information can help in further analysis of third-party, and enable organizations to take appropriate and timely actions.

4 Leverage external content

While internal screening assessments, onboarding, risk assessments, continuous monitoring are critical to third-party due-diligence, it is also important to take information from outside the organization. Multiple organizations today prefer to validate their third-party via external data sources like credit ratings, sanction lists and adverse media. This provides a complete assessment of third-party risks. While this can be done manually, it becomes burdensome even if conducted for a small set of critical third-party, thus technology can be used to automate this activity and provide relevant intelligence quickly.

5 Establish a well-defined escalation process

While each activity from the time of onboarding a third-party helps mitigate likely risks, the risks cannot be avoided completely. Additionally, the pressure from regulators has increased to document the process of identifying, reporting, investigating, and escalating incidents. Thus, an escalation framework is critical to resolving issues by expediting the decision-making process.
Conclusion

Ensuring business growth while adhering to regulatory mandate, and addressing customer needs requires organizations to establish the right balance between the decision to outsource and ability to manage third-party.

Each organization is dependent on a third-party network, and the viability, capability, and agility of this network dictates success within a constantly changing business landscape. However, depending on third-party also poses multiple risks to the associated organizations. Accountability for non-compliance by any third-party lies with the associated organization.

The proactive due-diligence of a dispersed, multi-layer, complex third-party network is an uphill task, but a vital one. Embedding a culture of compliance across the supply chain is an end goal worth achieving. One of the steps toward this will be to establish a robust third-party due-diligence program, consisting of third-party screening and onboarding procedures, risk assessments, ongoing monitoring, and corrective or preventive actions.

- Enhance compliance with the full range of third-party management regulations including OCC, HIPAA, FCPA, the UK Bribery Act and the Dodd-Frank Act