Third-Party Risk Management:

Building Relationships with Confidence

Effective third-party risk management (TPRM) – the process by which an organization manages and continually monitors its relationships with its vendors, distributors, resellers, and other agents and intermediaries – is increasingly becoming a vital part of an organization's compliance portfolio.

Largely driven by an unprecedented growth in the complexity of regulatory requirements and the maturation of environmental, social and governance (ESG) concerns, organizations are now expected to look beyond their own operations and ensure their third-party relationships account for forced labor and other human rights abuses. While historically, TPRM has been viewed as an ancillary compliance concern largely addressed by means of written questionnaires and reliance on standard contractual provisions, the emergence of a new regulatory climate demands a novel approach to TPRM; an approach characterized by building and sustaining a relationship of mutual trust between the primary contracting organization and the third parties it enlists to provide goods or furnish services.

By shifting the focus from conventional criteria to a more holistic approach to TPRM, organizations can ensure their risk management practices remain malleable and susceptible to evolution – fundamental characteristics in an age of rapid regulatory change. Viewed in this light, TPRM becomes more than a mere 'check the box' exercise. Instead, both parties benefit from building a lasting collaborative relationship meant to engender both consumer and regulator confidence.

Reputational and regulatory risk

Conventional risk management practices in the realm of reputational risk typically rely on both preliminary and recurring screenings to identify potential areas of concern. Under this model, the primary contracting organization assumes the responsibility of investigating the third parties on which it relies for any evidence of malfeasance or operational irregularities that could reflect negatively on that organization.

Reputational risks are then assigned an appropriate weighting based on the nature of the issues identified, with more routine reputational risks (*e.g.*, modest monetary penalties and fines imposed by a regulator) being afforded less of a weighting than major risks (*e.g.*, a history of regulatory infractions with a direct bearing on the third party's ability to discharge its obligations to the primary contracting party).

In a similar vein, current practices focused on risk mitigation from a regulatory compliance standpoint tend to emphasize adherence to a fixed universe of laws and regulations with third parties required to certify they maintain appropriate policies and internal controls that sufficiently address anti-bribery and corruption risks and sanctions and export control risks, among others. But these static models are outdated in an environment where trust is an essential underpinning of any contractual relationship.

Accordingly, a more appropriate risk mitigation strategy in this area is thorough evaluation of the prospective third party, its culture, reputation, and remedial capacity, at the very inception of the business relationship and periodically thereafter. While reliance on standard due diligence questionnaires is still part and parcel of this evaluation, contemporary organizations are required to venture outside of such standard techniques and **truly understand how the third party partner operates in practice**.

This necessarily encompasses a more meticulous examination of the third-party partner's policies and procedures than conventional risk mitigation measures currently require. Thus, in addition to requiring the third-party partner to disclose its code of conduct/ethics and internal reporting policies, a conversation with the principal contracting organization should be held that emphasizes how the paper-based compliance program is actually operationalized. For instance, rather than requiring a third-party partner to certify senior management is committed to the principles underlying the compliance program, the principal contracting organization should ask the third party to demonstrate how management commitment is emphasized.

Additionally, candid conversations should be held between the parties with respect to any deficiencies that might currently exist in the third party's compliance program in addition to any remedial measures the third party has undertaken in response to either the results of a routine audit or a regulator inquiry. In this instance, the goal should be to assist the third party with the overall enhancement of its compliance capabilities as opposed to merely passing judgment. By shifting the focus from mere self-interest to mutual dependency, both the principal contracting party and its third party partners can focus on building capacity to meet both current and emerging expectations.

Finally, careful attention should be given to an organization's supplier-specific code of conduct that eschews a one-size-fits-all approach. A better approach is a flexible regimen that accounts for the unique risk factors faced by each category of third parties with whom an organization contracts. Here, the emphasis should be on adopting a concrete series of third-party expectations that account for major risk factors based on third party role. In the case of distributors and resellers, this includes observance of antitrust laws and regulations that forbid price fixing and other forms of anti-competitive activity. Conversely, in the case of intermediaries and other agents – especially those expected to interface with foreign governments on the principal contracting organization's behalf – the focus may well be on adherence to anti-bribery and corruption regulations.

Operational risk

While the assessment of operational risk typically revolves around the activities of the principal contracting organization itself, such risks can also arise in the context of third-party relationships.

> *By shifting the focus from mere self-interest to mutual dependency, both the principal contracting party and its third party partners can focus on building capacity to meet both current and emerging expectations.*

Here, operational risk refers to the totality of factors that could impede a third party from delivering the goods or services it contractually commits to providing in the context of any definitive agreement. These risks include, but are not limited to, human errors, design flaws, system failures, internal fraud, and natural disasters. In each instance, the capacity of the third party to meet its obligations to the principal contracting party is significantly impaired.

In the contemporary marketplace, operational risks can completely frustrate the ability of the organization – often heavily reliant on the work of third parties – to deliver tangible goods to its customer base, thus jeopardizing the organization's very existence. While operational risk in a third party context has typically involved an independent assessment of the vulnerabilities facing such parties in relation to the overall business objectives of the primary contracting party, a more nuanced approach to risk management in this domain is required. As with reputational and regulatory risk, this approach should be centered on building a relationship of trust that addresses the unique operational risk profile of the third party in question.

In that vein, attention should be paid to emerging risk factors like data privacy and cybersecurity, which carry the potential for inflicting significant, even crippling, damage on third parties compromised by unscrupulous actors. To reduce the likelihood of data breaches and cybersecurity mishaps, it is important for the primary contracting organization to understand what security measures each third party has adopted and whether those measures are sufficient to prevent the most serious cybersecurity violations from occurring in the first place.

Moreover, operational risks should be addressed in the context of any definitive agreement reached with third parties. By relying on customized contractual representations and warranties, organizations can direct the focus of the third party to major vulnerabilities that should be remediated in connection with the establishment and maintenance of a business relationship.

For instance, if a third party has a weak information security infrastructure, the contracting organization can draw attention – and consequently resources – to that particular vulnerability by having the third party commit to adopting specific technological safeguards. Here, the focus should be on assisting a third party with identifying and proactively addressing vulnerabilities before they are exploited, rather than merely identifying causes for contractual termination. As the relationship between the parties matures, these provisions can be modified by addendum or amendment to address other deficiencies that could negatively impact the contracting organization's ability to function as a going business concern.

ESG risk

Perhaps more than any other risk domain, the rise of ESG concerns in the form of forced labor, human trafficking and other human rights abuses naturally lends itself to collaboration between the parties in the form of identifying and ending such abuses wherever they may occur in the value chain.

As regulators move to adopt increasingly more stringent supply chain laws and regulations requiring enhanced due diligence on the part of principal parties, cooperation with third-party partners is part and parcel of appropriately addressing emerging threats. However, rather than aligning the organization's third-party risk management strategy with particular ESG concerns, organizations can adopt a more flexible approach to TPRM by carefully considering all potential ESG risks that might arise in the context of a particular third-party relationship.

Continuous communication between both the principal contracting organization and its third-party partners maximizes the potential that such risks are promptly addressed. Thus, in the case of a third party that operates in jurisdictions known to employ forced labor, both entities can collaborate in devising a strategy for the timely elimination of that abuse before it materializes into an actual threat.

Adopting a more dynamic approach to TPRM benefits both the principal contracting organization and all third parties with whom it interacts by shifting the focus from addressing static concerns to identifying and sufficiently addressing actual threats. This not only enhances the quality of the relationship between the parties, but also manifestly demonstrates the parties are committed to operationalizing compliance concerns in the context of proactive TPRM.