NAVEX®

Checklist

VOLKOV

10 Steps to Implement a Defensible Third-Party Risk Management Program

1. **Clearly define and describe the extent of the organization's risk tolerance.**

Consider the industry and various jurisdictions in which your company operates in connection with the company's own risk tolerance threshold. Are there specific risks inherent to conducting business in a particular economic sector, country, or region? Has the company carefully identified these risks during the risk assessment process? What mitigative or other precautionary measures has the company agreed to implement to address these risks?

2. **Prepare and adopt a third-party risk management (TPRM) policy that sets forth the procedure the organization will employ to properly vet, onboard, and where necessary, disengage suppliers.**

The organization should adopt a specific policy that serves as the foundation for third-party risk management throughout the organization and its various operating units. The policy should set forth, in detail, **the process used by the organization to *identify, screen, select, evaluate* and *monitor* prospective suppliers.**

Ideally, the TPRM policy should also include a *business partner code of ethics or conduct (the Code).* At a very high level, the Code should set forth the organization's expectations concerning acceptable conduct. All third parties with whom the organization contracts should be bound to observe the Code. A breach of the Code should be immediate grounds for contractual termination.

The TPRM policy should also establish *roles and responsibilities* with clarity. This includes identifying which business units or individuals will be responsible for the execution of particular policy components such as vendor/supplier selection, initial denied party screening, contractual negotiations, audit/inspection, renewal and termination, etc.

3. **Assign a risk rating to each third party utilizing an appropriate scale.**

A TPRM scale should clearly segregate risks into three primary categories – *high risk, medium risk, and low risk* – and rely on objective criteria to assist the compliance function in identifying the most critical risks facing the organization holistically.

Third-party resources – such as Transparency International's Corruptions Perceptions Index ("CPI") – can streamline this process with respect to particular areas of concern. A composite score, accounting for the full view of risks the organization identifies as relevant, should then be calculated for each vendor. Discretion is crucial in ensuring only a small percentage of risks are actually classified as high risk, which enables the company to more effectively allocate resources for risk mitigation measures.

4. **To the extent possible, map the entirety of the company's supply chain to maximize visibility into the full product/service lifecycle and visually identify where the greatest risks lie.**

While this may seem like a tedious task, collaborating with knowledgeable internal stakeholders to understand what contributions various third parties make to the company's product/service lifecycle is an indispensable component of contemporary TPRM practice. This is particularly true where the company may be subject to regulatory schemes like the European Union Corporate Sustainability Due Diligence Directive, German Supply Chain Act, or the Uyghur Forced Labor Prevention Act, among others.

In each case, mapping the supply chain is required to identify non-compliance with prescribed environmental and/or human rights standards. From an enterprise risk perspective, mapping can also aid the organization in concretely identifying and addressing operational vulnerabilities that might arise from reliance on a particular third party.

5. Select and implement an automated TPRM system for utilization in connection with the administration of the TPRM program.

For all organizations, the management of third-party relationships requires the utilization of an **automated TPRM solution** that consolidates TPRM administration functions into a single platform. Reliance on manual processes is both insufficient and unlikely to meet current regulator expectations, which place a considerable emphasis on the ability of the organization to conduct due diligence, administer training, avail itself of audits, issue compliance certifications, and align enterprise and compliance risks effectively.

This necessitates adopting an automated solution such as the NAVEX One Governance, Risk, and Compliance Information System (GRC-IS), which allows the compliance function to onboard, screen, prioritize and monitor vendor risk information in real-time.

6. Review all standard forms of agreements typically utilized with the organization's suppliers and vendors to incorporate key compliance covenants, representations, and warranties.

A key component of effective TPRM is the delineation of clear contractual standards in the context of any definitive agreements reached between the primary contracting organization and third-party partner.

In addition to being bound by the organization's Code, the contract itself should require the third party to permit the audit and inspection of its books and records upon reasonable notice. The contract should also provide for the invocation of termination rights in the event the third party fails to comply with the Code or any substantive provision of the definitive agreement calling for the observance of particular laws or regulations.

7. Consider providing training to third party partners in the areas of great concern.

The provision of training to third parties is a convenient means of emphasizing that the primary contracting organization takes its compliance obligations seriously. To that end, training can be offered by the organization to its third-party partners in the highest risk areas identified during the third-party screening and onboarding process. For instance, in a country with a lower-than-average CPI score (indicative of systemic corruption), targeted training in the form of exposure to anti-bribery and corruption (ABAC) principles would reinforce the message that the corporation has no tolerance for illegal attempts to influence third parties through the payment of bribes or the provision of gifts.

8. Ensure third parties are able to report violations of the organization's Code or other ethical and legal infractions.

Where feasible, companies should consider leveraging their existing incident reporting system to allow external parties – including the employees of any business partner – to report on matters implicating a breach of the Code or other ethical and/or legal infractions by the corporation's employees, contractors and agents. This reporting capability is increasingly required by regulatory schemes focused on supply chain transparency.

9. Prevent, to the great extent possible, the fragmentation of third-party information.

Perhaps the greatest challenge facing contemporary companies is the consolidation of existing information silos. To be effective, all information pertaining to a particular third party should be stored in a single location that is widely accessible by key organizational stakeholders. Access to a complete file containing supplier information is critical to maintaining a reliable risk profile.

10. Periodically review and update TPRM policies and procedures in light of regulatory developments and lessons learned.

It goes without saying that the organization should revisit its own policies and procedures relative to TPRM on a regular basis to make improvements based on lessons learned and on emerging regulatory expectations. To maximize the effectiveness of the TPRM program, policies and procedures should be revisited at least annually, if not sooner, to ascertain whether any modifications are needed.