

The Complete Compliance and Ethics Manual 2024

Appendix 5-C: Best Practices Checklist for Managing Third-Party Risk

Below is a checklist of best practices for reducing the risks posed by the third parties your organization may do business with. While every third-party will pose some amount of risk to your organization, this risk can be reduced by taking these steps.

Stage of Engagement	Risk Mitigation Measure	Achieved
Prior to Selection	The legitimate business purpose for seeking a third party has been carefully demonstrated, documented, and approved by the organization in advance of such third party being hired or retained with careful explanation of why no currently existing company resource or third party is sufficient.	☐
	Newly requested third-party relationships in high-risk countries, or where activities involve regulated or high-risk operations, are reviewed and approved by the organization's chief ethics and compliance officer or other designated company official in advance.	☐
	Slate of potential third parties to fill identified need are screened for Office of Foreign Assets Control sanctions compliance to eliminate any prohibited parties.	☐
	Assessment of risk of human trafficking and forced labor in the supply chain for the services to be provided should be performed. If there is a high risk of trafficking or forced labor, a written risk mitigation strategy and tactics should be established in advance.	☐
	The organization has a code of conduct in place applicable to third parties or a requirement that third parties have their own code with content approved by the organization as being substantially similar to that of the organization.	☐
	Organization has a widely publicized and readily available global reporting helpline and process available in all local languages through which employees, contractors, third parties, agents, etc., can seek guidance, report concerns, and ask questions (anonymously if desired).	☐

	All of the organization's employees working with third parties have been trained and are fully knowledgeable of applicable anti-bribery, anti-corruption, and US Foreign Corrupt Practices Act compliance standards.	☐
	The organization's employees working in supply chain, procurement, accounting, senior and local management, legal, and compliance have been trained on third-party risks and compliance standards and can readily and correctly identify potential red flags.	☐
	All third parties, including their owners, officers, and managers are reviewed for potential conflicts of interest prior to being engaged.	☐
	The specific terms of engagement for a third party, including proposed compensation and/or commission structure and rate, is reviewed by legal counsel to ensure compliance with local legal requirements and to ensure the amount of proposed compensation is consistent with the rates of compensation paid to other third parties for similar services and in similar locales.	☐
At the Time of Selection and Contract Execution	Ownership of final proposed third-party candidate is verified through beneficial ownership and anti-money laundering checks to ensure candidate is viable.	☐
	Final identified third-party candidate and its owners, officers, and managers are screened for Office of Foreign Assets Control sanctions compliance to ensure they do not appear on any denied or prohibited party list.	☐
	The organization performs detailed, risk-based due diligence on final identified third party, including their owners, officers, and managers, to look for potential red flags, including negative news or reputation, enforcement actions, penalties, fines, and litigation. It verifies such third parties are actually qualified and have the requisite capitalization employees, resources, and experience needed to provide the services or deliverables they are being retained to provide. Diligence scope and depth will vary based on risk of proposed transaction (e.g., geography, type of services).	☐
	Organization provides information to third party to address how the code of conduct will be formally applied and enforced in relation to third parties.	☐
	Owners, officers, and managers of the third party certify in writing that they have received, completed, understand, and will comply with the organization's anti-corruption/anti-bribery policy and training.	☐

	Owners, officers, and managers of the third party certify in writing they will not engage in human trafficking, forced labor, or child labor practices.	☐
	Owners, officers, and managers of the third party certify in writing that they have read and understood the organization's code of conduct or affirms their agreement to comply with their own substantially similar code.	☐
	Owners, officers, and managers of the third party certify in writing that neither they nor their family members or close associates have any undisclosed or prohibited conflicts of interest.	☐
	Owners, officers, and managers of the third party certify in writing that they are not current or former employees of the government.	☐
	Third-party service agreement contains provisions making compliance with the above requirements a condition precedent to payment under the agreement and allowing for immediate termination of the agreement in the event of a reasonable belief on the part of the organization of any violation of policy, code, regulation, or law.	☐
During the Term of the Engagement	The organization provides its third parties with periodic, effective training and communications (in local language) on its standards, culture of compliance, and other legal requirements.	☐
	Third parties, including their owners, officers, and managers, recertify in writing on an annual basis that they have received, completed, understand, and will comply with the organization's anti-corruption/anti-bribery policy and training.	☐
	Third parties, including their owners, officers, and managers, recertify in writing on an annual basis that they have read and understand the organization's code of conduct or reaffirm their agreement to comply with their own substantially similar code.	☐
	All third parties, including their owners, officers, and managers, complete annual written conflict of interest recertifications.	☐
	The organization renews its due diligence on the third party, including its owners, officers, and managers, on a predetermined and risk-based cadence. High-risk third parties require renewal of due diligence using a shorter cadence than low-risk third parties.	☐

	The organization pays its third parties only using standard payment protocols established by the company (e.g., direct deposit).	☐
	Third-party activities are closely monitored by the organization's management in all operating locations.	☐
	Third parties are directly supervised and managed by the organization's employees in high-risk operating locations.	☐
	The organization provides third parties with support and guidance in mitigating its compliance risks.	☐
	The organization conducts regular and ongoing audits of third-party sites and operating locations for all business activities. Audits include review of books and records, risk assessments, site visits, management and employee interviews, and supporting document review.	☐

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase](#) [Login](#)