COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2024
Third-Party Risk Management: The Who, What, Why, When, and How

By Veronica Pickens, CHC, CCP[1]

Who Does It Apply to and Impact?

Third-party risk management (TPRM) applies to any organization that uses external parties such as contractors, suppliers, distributors, or vendors to conduct or provide services on their behalf. As you can see, this affects most organizations in some shape or fashion around the globe. Think about the organization that you are employed by. Does it have any contractors, suppliers, or vendors in place that your organization is reliant upon to keep the office running administratively, or do these third parties provide the software or hardware needed to effectively produce, sell, and maintain your products and services to your customers? Your response to this question was most likely a resounding yes, as it would be for most people.

Unfortunately, stakeholders in most organizations often do not fully understand the impact that third-party relationships could have on performance and sustainability. When third-party relationships are not managed appropriately, the stakes are exceedingly high for an organization—and ultimately its customers. In 2020, Deloitte published its fifth annual global survey on extended enterprise risk management (EERM), another term for TPRM.[2] This survey included 1,145 participants from 20 countries around the world and covered all major industries.[3] Key findings from this survey—which unfortunately took place before the pandemic, so it wasn't influenced by the drastic shifts of 2020—were as follows:

- Organizations are growing increasingly concerned about the rising costs of getting TPRM wrong, as there is a growing trend of reliance on third-party relationships with contractors, suppliers, or vendors that are carrying out critical mission functions for organizations. This, of course, elevates the risk and exposure to those organizations.
- Organizations are more aware of the need to be responsible as a business; however, their budgets for TPRM do not reflect such responsibility. TPRM is not being funded at a strategic level and, as such, most likely will not adequately have all the requisite controls in place to understand and mitigate risk related to the third-party relationships.
- A rise in regulatory activity related to TPRM has put pressure on organizations because the bar is being raised on what is perceived as a "mature" program. Ultimately, this means that organizations must do more or run the risk of not being able to demonstrate appropriate oversight if and when things run afoul due to a third-party relationship.
- Organizations have struggled to stay abreast of the constantly evolving technology for TPRM and are particularly concerned about the lack of seamless integration of such technologies. Survey respondents reported being dissatisfied with their current TPRM technology as they are planning for a longer-term outlook that focuses on efficiency and effectiveness. This area is seen as a gap or risk.
- A trend was demonstrated in which organizations are exploring and engaging with external resources to help evolve their TPRM programs.

- Although many senior executives are broadening their focus of TPRM beyond risk, they are struggling to coordinate their approach and access the necessary decision-making data promptly.[4]

Additional details from this survey as well as one published by Ernst & Young Global Limited will be shared as part of this article. Both surveys provide invaluable information related to TPRM and are being recommended as supplemental reading materials to further your education on TPRM.

What Is TPRM?

TPRM is the process of identifying, assessing, and controlling risks presented throughout the life cycle of an organization's relationship with any of its third parties (e.g., vendors, suppliers, distributors).[5] Organizations are tasked with dealing with their internal risks. However, when there is outsourcing or reliance on third parties, organizations also have to understand the risks that those third parties could potentially have on their organization and then take steps to minimize the impact of such risks through various processes. Ultimately, there are inherent risks for any organization when it has third-party relationships, but an organization should make every effort to be aware of what those risks are, the potential impact, and have documented remediation processes in place.

TPRM processes should begin during the procurement process with third parties and then extend through the end of the offboarding process. Anything less poses risk for your organization. As part of the initial due diligence and throughout the life cycle of third-party relationships, risk types that should be part of the evaluation may include:

- **Strategic**: Risk that occurs due to adverse business decisions or the failure to implement appropriate business decisions in a manner consistent with stated strategic goals. An example of a strategic risk is if a company's business model is to be the low-cost provider of a product or service, and a competitor from a low-wage country suddenly enters the market, thus destroying the original company's value proposition.

- **Reputational**: Risk that occurs due to negative public opinion of an organization. An example of a reputational risk is the Wells Fargo cross-selling scandal. In September 2016, this financial institution, which had been ranked 7th on *Barron's* 2015 list of the "Most Respected Companies," fell from public grace a year later when it announced that it would be paying $185 million to settle a lawsuit filed by regulators and the city and county of Los Angeles. This institution admitted that as many as 2 million accounts were opened without customer authorization over five years.[6] Over the course of the next two years, comprehensive investigations by various regulators ensued, resulting in this institution agreeing to a $1 billion settlement with the Consumer Financial Protection Bureau and the Office of the Comptroller of the Currency to resolve auto and mortgage lending violations; a $480 million settlement for a securities class-action lawsuit over cross-selling; and settlements totaling $575 million with 50 state attorneys general to resolve civil claims for cross-selling, auto lending, and mortgage lending violations.[7] This institution, which had been known as a trustworthy organization, put financial gain in front of the culture and value that it had built.[8] This adversely affected shareholder value, as well as customer trust and confidence.

- **Operational**: Risk that occurs due to loss created by inadequate or failed internal processes, people, systems, or external events. An example of an operational risk was shared by McKinsey & Company in an article about a global bank that tackled unacceptable false-positive rates in anti-money laundering (AML) detection.[9] The results were as high as 96%, causing significant concern and potential risk to the organization. The institution then used machine learning to identify crucial data flaws and made the necessary data-quality improvement, resulting in an elimination of an estimated 35,000 investigative

hours. Fortunately, it had processes in place that were monitoring this risk and were able to course-correct before any damage was done. Although this article was specific to the financial services industry, it contains best practices that can be applied across industries and, as such, is recommended as a supplemental read.

- **Transactional**: Risk that occurs due to problems with service or product delivery. An example of a transactional risk is if a company missed a forecasted product launch date. Because the launch did not happen as planned, customer orders were delayed, creating a negative customer experience and lower revenue. Another example would be losses due to foreign exchange rates when companies are importing goods and services. Adverse changes in the market lead to reduced profit margins and other implications.
- **Compliance**: Risk that occurs due to violations of laws, rules, or regulations; intentional and inadvertent noncompliance with internal policies or procedures; or violations of the organization's business standards. An example of a compliance risk is the violation of a regulation such as the False Claims Act,[10] where a company fails to report an overpayment from the government that is later uncovered by a regulatory body. Another example is if company engages in activities that violate the Foreign Corrupt Practices Actby paying funds to a foreign government official to obtain special treatment for its business.[11]
- **Information security**: Risk that occurs from unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. An example of an information security risk is SolarWinds, a major US information technology (IT) firm. The US government and many US-based corporations were shaken in 2020 when news of the cyberattack on SolarWinds hit the airways. In early 2020, hackers secretly broke into SolarWinds' systems and added malicious code to its Orion software, which went undetected for more than nine months.[12] Orion is widely used by companies to manage IT resources. Unbeknownst to SolarWinds, it sent out software updates to its customers that included the hacked code. This code created a backdoor to customers' IT systems, which hackers then used to install even more malware to spy on organizations, including several US government agencies. Just think about the potential privacy violations that occurred because of this cybersecurity breach. It will take years for the effects of this attack to be undone and for affected networks to be secure again.

As you can see from these examples, the various risk types can't be ignored by organizations, and overall risk is compounded when organizations rely on third-party relationships. Therefore, establishing a comprehensive TPRM program that is both effective and efficient is essential.