Plugged In: Putting a sharper focus on third-party risks

October 27, 2020

Power and utility (P&U) companies increasingly rely on third parties to deliver critical products and services to their clients and customers. Although third parties—which include vendors, contractors, and other counterparties—provide countless benefits, they also expose companies to unforeseen risks. COVID-19 only underscored how unforeseen events can affect third-party relationships.

P&U companies are particularly susceptible to cyber security and customer data-privacy risks, as well as risks related to greenfield and brownfield construction projects and operational maintenance. Any failure by a third party can mean added costs as well as reputational damage.

That's why P&U companies need a clear strategy and framework for the selection, approval, and ongoing management of third parties. That strategy needs to be supported by a proper third-party risk management program (TPRM) so the organization can adequately assess and proactively manage the risks posed by third parties.

A recent KPMG survey, however, found that P&U companies face challenges in creating effective and scalable TPRM programs. According to our survey, only 27 percent of P&U respondents said that they were highly proficient in developing a comprehensive understanding of the risks posed by a third party.

Clearly, there is a need to take a closer look at their third-party strategy and program to help ensure these risks are identified, prevented (or at least mitigated), and responded to without impeding business objectives.

What follows is a closer look at specific third-party risks that P&U companies face.

Cyber and privacy risks

Public utilities provide people with vital services, so a cyberattack can cause a major disruption to a population. Utilities may also be the sole provider of a service for a given region, and therefore possess large amounts of sensitive private information.

News reports show that public and private P&U companies have reported that cyber intrusions and attacks are increasing both in frequency and complexity. Despite their own best-designed and most effective controls, they are also impacted by the unintended consequences of third parties' failures or lapses, as well as those third parties' relationships. Given these realities, cyber risks and related data privacy and data protection concerns remain a critical consideration around third-party risk.

In fact, according to KPMG's survey, 41 percent of P&U respondents said that cyber risk was driving TPRM activity and 34 percent cited data governance and privacy. Of concern, however, is that only 28 percent of energy respondents said that their organization was highly proficient in identifying and fixing vulnerabilities in their cyber defenses.

The implications of cyberattacks and private data breaches can lead to business interruption and failure to meet public requirements and client needs, as well as the theft or loss of sensitive company data, including private information about employees, customers, vendors, and other stakeholders. Likewise, there are the monetary and reputational costs, including loss of revenue, expenses to remediate, penalties from compliance and regulatory failures, litigation and damages, and, not least of these, reputational damage and impaired trust.

Given the potential fallout from a cyber incident, it is interesting that only 31 percent of respondents identified protecting brand reputation as guiding TPRM activities; and only 25 percent identified business continuity/disaster recovery as an impetus for TPRM activities. That said, the ability to mitigate and respond to cyber risk has downstream benefits.

Construction and maintenance third-party risks

Under the current market conditions, there is greater emphasis on return on investment and maintenance of financial viability for expenditure on brownfields and greenfield P&U projects. In addition, cost optimization priorities are driving increased risk tolerances for over planned maintenance activities and third party outsourcing. Since this engineering, construction, and maintenance work is typically performed by outside contractors and suppliers, P&U companies need to pay close attention to third-party risks related to the agreed contractual obligations, including related regulatory compliance requirements (e.g., safety).

For construction projects, the key is understanding the associated risks and aligning the commercial strategy and execution approach. Planned and unplanned maintenance is part of day-to-day operations and should be linked to clear risk-based preventative maintenance framework, particularly with expanding accountability beyond the core operations into areas such as vegetation management to ensure safe and efficient operations. These risks can include responsibility for liabilities arising from accidents and injuries, cost overruns, missed project milestones, reliance on subcontractors and quality of work. There is also the risk of the P&U company not effectively monitoring cost and schedule for agreed scopes of work, which could lead to excessive costs and regulatory compliance exposure. P&U companies will need to evaluate their own risk tolerance against the size and type of project or maintenance program they are planning, the availability of resources and technical skills in the market, as well as the experience and capacity of the third party to ensure successful delivery and execution.

Framework for an effective TPRM

Given these risks, among others, P&U entities need to balance the need to effectively manage risk across their third parties, while also meeting the needs of the relationship owner and other stakeholders within the business. TPRM programs should focus on the ongoing management of third-party relationships, the performance of the third parties, and the continued validation of third party's compliance with control environmental expectations.

TPRM operating model

An effective TPRM operating model is based on four pillars:

Governance

— Policies, standards, and roles and responsibilities throughout the program and third-party lifecycle

Process

— Consistent procedures and execution across the TPRM program

Infrastructure

— Technology that ensures efficient workflow, task automation, consistency, reporting, and audit trails

Data

— The collection, retention, and accessibility of real-time data of the program's activities.

Final thoughts

Third parties, while increasingly necessary, can expose organizations to new risks that can be costly and threaten business reputation. The use of third parties doesn't transfer the associated risks; it changes the way the key risks are managed. Indeed, as organizations adjust to global events and economic uncertainly, the need for more robust and sustainable TPRM programs may be more important than ever. Our research shows that P&U companies may need to reevaluate their third-party programs and processes to account for new risks and challenges—as well as relationships themselves. With increasing cyber threats and other vulnerabilities, and reliance on third parties, P&U companies need to make TPRM a strategic priority to help ensure business continuity and resiliency.

For more information

For more information about third-party risk management, or to read the KPMG Third-Party Risk Management outlook 2020, please visit our website, Navigating Third Party Risk.

KPMG Global Energy Institute

Launched in 2007, the KPMG Global Energy Institute is a worldwide knowledge-sharing forum on current and emerging industry issues. This vehicle for accessing thought leadership, events, and webcasts about key industry topics and trends provides a way for energy executives to share perspectives on the challenges and opportunities facing the energy industry, arming them with new tools to better navigate the changes in this dynamic arena. To receive timely updates and insights relevant to the P&U industry, register for the Global Energy Institute.

Contact us

Travis Canova
Director, Advisory
KPMG in the U.S.
E: lcanova@kpmg.com

Hayden Love
Director, Audit Assurance Risk
KPMG in Australia
E: hlove@kpmg.com.au

Lucie Wuescher
Managing Director, Advisory, Internal Audit & Enterprise Risk
KPMG in the U.S.
E: lwuescher@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/socialmedia