Rethinking risk: Trends in third-party risk management (TPRM)

Like most business ecosystems, TPRM is also evolving rapidly. The dependence of organisations on third parties for products and services to effectively innovate, scale and grow their business is on the rise. As a result, organisations' exposure to risks increases with every product and service procured from and in collaboration with external entities. It is essential for organisations to understand and manage the risks that arise due third parties – whether they are distributors and resellers, consultants, agents, partners or vendors. Therefore, it is crucial to have a system in place that is commensurate with the increased risks faced by an organisation and its supply chain network.

Managing third-party risks is important in order to have a functional business. While assessing the risks, it is essential to understand issues such as business integrity, reputation management, licencing, human rights and environmental violations. These risks can collectively, or individually, jeopardise an organisation's brand identity, reputation and profitability. To this end, we have enumerated some of the key risk trends that organisations need to recognise and manage in order to excel in the challenging economic ecosystem below.

1. **Effective cyber defence in a digitally dynamic world:** As per PwC's 2024 Digital Trust Insights Survey, 85% of Indian respondents predicted that their organisation would increase their cyber defence budget.[1] The third-party entities that organisations were interacting with have now changed. Instead, there are various companies, such as cloud or hosting providers, that have helped in improving competence and convenience. However, as a result, they also have an increased exposure to many unexpected security risks. Cyber attackers, with their sophisticated technologies, are always searching for weak links in the business ecosystems of organisations, which are more often than not spotted in third-party systems. It is thus essential that organisations pay as much attention to this extended system and ensure that all the third parties they interact with are also brought within the organisation's cyber defence system.
2. **Environmental, social and governance (ESG):** Businesses form a fundamental part of our society since they play an active role in contributing to the creation and sustenance of a healthy ecosystem. There is a growing awareness of this aspect and, subsequently, companies are ensuring that they prioritise sustainability and follow responsible practices. While corporates have increased their focus on ESG performance and risks within their immediate circumference, they need to extend the same to their vendors as well. ESG aspects could include a vendor's labour practices, human rights record and carbon footprint, to name a few. With a continuously evolving business scenario, it is crucial that one includes ESG in an organisation's TPRM strategy since it is more of a business opportunity and less about safeguarding against regulatory action and reputational damage. Focusing on ESG demands can improve a firm's customer base, attract necessary investment opportunities and enhance brand reputation.

1 https://www.pwc.in/assets/pdfs/digital-trust-insights-india/digital-trust-insights-india.pdf

3. **Leveraging technology:** In the past, TPRM was an annual exercise that involved ticking off mandatory items from a list manually. While human intelligence remains indispensable and can't be replaced, firms need to focus on incorporating and using cutting-edge technology like machine learning, automation and artificial intelligence (AI). These technologies will help in accelerating the processes, reducing the inherent and resultant complexities, and pinpointing the blind spots on the supply chain. Moreover, they will enable an organisation to scrutinise its big data in order to recognise anomalies within financial data or equipment maintenance, or even in the selection of suppliers or vendors, and aid them in making more informed decisions and effectively respond to potential disruptions and prevent them.
4. **Geopolitical concerns:** Geopolitical conflicts around the globe play a key role in disrupting supply chains, thus placing an unexpected pressure on business continuity programmes and impacting the organisation's ability to find alternate sources for products and services at an accelerated pace. Such situations – local political unrest, civil unrest, new coronavirus strains or labour shortage – have a cascading effect on the availability of raw materials. It is therefore very important that organisations anticipate the geographical risk profile of their partners and map the third party's organisational structure – including their affiliate and subsidiaries, as well as the physical locations of all manufacturing and service operations. While monitoring geopolitical risks needs to be a constant and continuous activity, it is also important to have backups for one's supply chain in case of sudden disruptions.
5. **Regulatory and compliance requirements:** Due to geopolitical conflicts, increase in cybercrime and issues such as ESG gaining prominence, regulatory compliance will remain a key focus for the next few years. Due to various uncertainties, rules and standards have become more complicated and businesses are scrutinised more intensely. Therefore, organisations need to be constantly informed about the regulations that govern their industry and keep updating their policy and practices relating to TPRM. Due diligence on the regulatory aspects of third-party entities also needs to be a continuous process and not a one-off operation – especially with regulatory authorities tightening the scrutiny of third-party interactions.

How can PwC help

The TPRM ecosystem is evolving and becoming more complex by day. This requires organisations to ensure that they incorporate a robust TPRM strategy into their operations. Utilising a proficient TPRM service provider is the first step to safeguarding a business and ensuring that there is no reputational or financial damage to the organisation.

PwC's Global Intelligence team assists clients in identifying information that enables them to make informed decisions before entering or investing in new or known/unknown markets. We provide market leading advisory and managed services via our third-party tracker tool, vendor due diligence process or other third-party assurance solutions. The firm is committed to staying on the leading edge in how it delivers its TPRM services. Thus, we ensure that we manage third-party relationships throughout their lifecycle and across multiple risk domains – including information security, reputational risk, privacy, physical security and ESG.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us:

Puneet Garkhel
Partner and Leader, Forensic Services
Tel: +91 98203 20181
Email: puneet.garkhel@pwc.com

Surpiya Verma
Executive Director, Forensic Services
Tel: +91 98925 05706
Email: supriya.verma@pwc.com

Contributor

Ayan Roy

Editorial support

Rashi Gupta

Design

Kirtika Saxena

pwc.in

Data Classification: DC1 (Internal)

KS/January 2024 - M&C 30771