Building a better working world

The journey to third-party trust

The interdependencies between companies and third parties have grown both more complex and more essential to the smooth functioning of day-to-day business. Across the supply chain, firms might work in tandem with contractors, joint ventures, service providers, brokers, agents, consultants and others. But while organizations can farm out responsibilities for numerous functions, they cannot outsource the accountability.

Two-way trust is necessary in this interconnected era, and trust must be embedded at the beginning of every third-party relationship. But how much time and resources should be invested in risk management? Risk can never be eliminated entirely, so where is the point of diminishing returns?

> Among the Fortune 100, as much as 50% of a company's expenditures involve third parties.

Risks associated with third parties

- **Regulatory and compliance risks** are growing, as are the costs for noncompliance. Privacy regulations, labor laws and tax regimes are particular concerns in relation to third parties and their extended networks.
- **Financial risk** comes into play if the third party cannot continue to operate as a financially viable entity. The consequences can be dire, particularly if a company is single-sourcing from the third party.
- **Cyber and privacy risk** is the front line of digital risk across the entire network of direct and indirect business relationships. Breaches span the familiar (passwords and other sensitive data) to the insidious (the hacking of individual parts or components).
- **Business continuity and resiliency risks** include the existential threats regarding third parties. A break in continuity within the supply chain demands immediate attention, and the ripple effects are often widespread.
- **Geopolitical risk** has always been a threat, but there have been few eras when preparing for it was so tricky. Even as global economic interdependence increases, political disintegration (tariffs, the rise of nationalism, Brexit and so on) is also on the rise.
- **Operational risk** associated with a third party also puts business continuity at stake. Deficiencies in a third party's operations jeopardize service and product delivery, and pose a deep threat to the supply chain.

On average, a company loses 9% of its stock market value from a supply chain failure.
Source: TK.

- **Digital risk** related to third party's business processes goes hand in hand with opportunity. Smart factories and other innovations are adding measurable value to the supply chain, but the benefits must be balanced with the risks they introduce.
- **Reputational risk** must be addressed from many angles. Regulatory noncompliance, for instance, can lead to fines and other costs — but the damage to a company's reputation can be far more severe. The same is true of third-party digital risk, such as a privacy breach that makes headlines.
- **Strategic risk** is the risk that the organization's and third party's strategic objectives and values are misaligned. For instance, organizations that emphasize a commitment to diversity or those with close ties to their communities, such as health care providers, will want to work with firms that have similar perspectives.

Thirty percent of organizations experienced a breach caused by a third party within the past two years.
Source: Third-party risk management survey, 2019, EY.

Flexible risk management for an era of disruption

Third-party risk management must be flexible enough to deal with the changing needs of an organization. As a company grows and its use of third parties increases, risk management processes must scale easily. A modular approach can help firms target key risks and deploy risk management resources efficiently.

For many, risk management begins with a thorough inventory of relevant third parties and the risks they pose. This includes defining and weighting risk tiers with some degree of formality, and assigning risks to them. The next step traditionally involves deploying analytic models, approaches and processes to manage these risks.

If traditional contractual agreements around risk are too heavy, a company might find it more appropriate to mitigate and manage risk as it arises. A flexible, adaptable version of third-party risk management that recognizes disruption might be the best way to protect the organization without stifling innovation.

Six components to build third-party trust

To address the risks that third parties pose, companies must have robust risk management capabilities in place. These six components help form the foundation of an effective, efficient platform.

Oversight and governance

Governance defines a company's risk-management vision and provides direction for execution. It's crucial to embed this vision into all levels of an organization. When the board and senior management are involved, it's easier to get buy-in and integrate risk management into day-to-day processes.

If possible, a centralized risk-management structure is best because it reduces redundancies and can be managed holistically. In a similar way, companies are increasingly leveraging sector-based alliances and consortiums for repeatable, cost-effective, third-party risk management practices.

Policies and standards

Policies and standards establish clear roles, duties and expectations about third-party risk through all phases of the risk-management life cycle. Internal stakeholders must understand their responsibilities when engaging a third party, and the associated risks.

Policies must also include escalation protocols for noncompliance. Executive management should be responsible for enforcement, as well as an annual (at minimum) policy review.

A mature third-party inventory

Before a company can manage risks, it needs to know what and where they are. A single source of truth for third-party vendors is essential. This high-level inventory should categorize vendors according to their risk profile (new vs. existing, degree of criticality, scope of deployment and so on).

Going deeper, the inventory should also include information such as spend, contractual details, use of subvendors (wherever possible) and a summary of key risks for each third party. Because this information is dynamic, companies must also review the inventory regularly and update when needed.

Risk models

Leveraging the inventory, organizations should determine the risks that are relevant and the risk-management models to use. In the past, this might have meant assessing the risks of only the largest suppliers.

But in an era of digital disruption and transformation, companies should consider whether that's the best mindset. Many companies do business with startups that don't come close to meeting basic third-party risk criteria. Yet these innovators and incubators are often critical to a company's growth and competitiveness. Therefore, a more flexible version of third-party risk management for smaller tier 2 and tier 3 vendors might be a better choice.

Third-party risk processes

Effective third-party risk management spans the life cycle of the engagement: sourcing, due diligence, contracting, onboarding, monitoring and termination. Key actions included within each phase follow:

- Sourcing
  - Inherent risk assessment
- Due diligence
  - Risk assessments
- Contracting
  - Terms and service-level agreement review
- Onboarding
  - Documentation of exit strategy (as applicable)
  - Establishment of monitoring cycle, including risk and service management
- Monitoring
  - Risk management assessment and monitoring
  - Contract risk review
  - Issue management
  - Risk treatment (acceptance)
  - Action planning
  - Monitoring of issue remediation and risk treatment
- Termination
  - Exposure/closeout risk assessment

Emerging technology

Emerging technology, including robotic process automation, is introducing efficiencies into third-party risk management, a process that still relies on Excel spreadsheets and manual input in too many cases. In addition to its labor-saving benefits, automation enables real-time reporting so executives can assess common risk themes and align budgets accordingly. It also allows procurement and contracting to better judge risks at contract initiation.

This component of third-party risk management includes predictive modeling to identify areas of emerging risk, and visualization tools to promote better decision-making at the executive level. Organizations that invest in new technology will stay one step ahead of those that continue to rely on manual processes.

The scope and scale of third-party risks have never been larger, and the consequences of mismanaging them have never been greater. Third-party trust is an innovative, agile approach to risk management that delivers the right strategies and tools to handle the emerging threats related to digital, the increased scrutiny of regulators and much more.

Begin your journey to third-party trust here.

US SCORE no. 08405-201US
2002-3399899
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com