

Risk Angles Third-Party Risk

The use of third parties is nothing new — companies have worked with suppliers, outsourcers, licensees, agents, and the like for years. What has changed, however, is the frequency and scale of third-party use and the regulatory focus on how organizations are managing third parties to address the inherent risks.

Kristian Park, partner and leader of the Contract Risk and Compliance practice of Deloitte LLP in the United Kingdom, discusses the escalation in third-party risk and the ways organizations should be mitigating it — but often aren't.

The challenge

Q: Why is third-party risk escalating?

A: A few factors are in play. First, volume. During the recession, we saw many organizations push more of their business out to third parties in an effort to reduce internal costs across the extended enterprise. Higher volume, of course, can mean higher risk. Second: scrutiny. Regulators have become more focused on how companies are managing outsourcing and third-party risk in general, and the fines for violations have reached hundreds of millions of dollars. With those fines has come a third escalating factor: reputational impact. When millions of consumers are personally affected by a third-party system failure or security breach, or when a well-known company is heavily fined or repeatedly called out with regulatory MRAs (matters requiring attention), the reputation of the involved organizations can suffer. The free-flowing nature of information also plays a role here: decades ago, a disruption in a local country would likely have stayed local; today it can quickly become a global issue.

As a result of the escalating risk — and the escalating fallout when risk becomes reality — boards are paying more attention and asking more questions. The fact that in most cases, even in leading global organizations, it's rare for someone in the organization to have an overarching view of who the company is doing business with or the risks these third parties impose on the business is a tremendous concern. Today, like never before, boards are considering third-party risk a top strategic risk. However, that hasn't yet translated into clear accountability for third-party risk oversight, either from a single owner or a function. The Chief Procurement Officer has frequently been asked to lead this role, but that can lead to skewed emphasis on supply, rather than a broader enterprise-wide view considering alliance relationships, distribution partners, and the like.

The impact

Q: What's been the traditional approach to managing third-party risk and where is there room for improvement?

Examining the extended enterprise

A closer look

Kristina (Krissy) Davis, an Advisory partner in Deloitte & Touche LLP (Deloitte US) and leader of the Finance & Operations market offering within Deloitte US's Advisory practice, discusses how companies are approaching third-party risk identification, assessment, and mitigation.

The banking industry has been a leader in addressing third-party risk, largely due to the new OCC and Federal Reserve regulations released in late 2013, and is generally ahead of other industries in its practices. However, over the past two years, adoption of the 2013 COSO Internal Control – Integrated framework¹ has propelled companies in other industries to look at “outsourced service providers” (COSO's term for third parties) and how they impact risk assessment, controls, monitoring, and the flow of information. In 2014, the COSO-driven focus on third parties was in the context of financial reporting; in 2015 we are starting to see the focus shift to operations and compliance.

In that time, concern about third-party risk has risen much higher in many organizations. Senior leaders and boards have recognized it as a strategic risk and made it a priority to proactively manage third-party relationships rather than reacting to a specific event. An initial challenge for organizations is to think more broadly about their third-party relationships, going beyond those “first-tier vendors” to include the second and third tiers as well.

The definition of “third party” is also expanding to include service providers within the organization. Inter-affiliate service providers are increasingly a focus of regulators, particularly those that supervise entities outside the country of the parent. Financial institutions are beginning to implement programs to provide a level of control that is similar to what they have in place for typical external suppliers. Internal service providers are also a key concern of the Recovery and Resolution Planning process, which has prompted banks to look at the details of their operation with an eye to reducing market impact in the event the banks come into financial stress.

A: Third-party risk has typically been addressed in a siloed fashion, with individuals in the organization looking at specific risks, usually within the supply chain. For example, in the banking sector, the focus might be on the IT department and the data protection issues and risks of sharing data with third parties. In the consumer products sector, the focus might be on risks to product quality and safety, with an eye to both protecting end users and safeguarding the company's reputation. While organizations have been right to be proactive in managing risks to certain functions or aspects of the business, many haven't pulled back from this narrow view to examine the broader business exposure — the holistic view that's essential to understanding overall risk exposure resulting from third parties and managing it enterprise-wide.

It's interesting to see how different levels of management within the organization have differing perspectives. For example, Chief Procurement Officers will often tell me third-party risk is being managed and is under control. Managers below them will likely say they're not 100% sure, but they know that certain risk areas are covered. Leaders above, such as others in the C-suite and the board, are usually much less optimistic and perceive third-party risk as a serious problem that's not being properly addressed.

The strategy

Q: What are leading companies doing to manage third-party risk?

A: Many companies are on a journey, and while some are further down the path toward robust third-party risk management, there are many that have not yet arrived. The first step is often the biggest stumbling block — getting visibility into who the company is doing business with. Once companies have some visibility, they start to think about how to manage the risk associated with these third parties they've identified, concentrating their efforts on those that pose the highest risk. It's more of a proportional response rather than a holistic one.

A thorough approach typically includes a framework and defined process for assessing third-party risk, such as a questionnaire that goes out to third parties and a means to score potential risks based on their responses. There would be strong governance in place to define next steps once a risk is identified, including guidance not only for remediating it but also deciding if it should be accepted and how to properly manage it if it is. There would be clear ownership of third-party risk, and people in the organization with a risk management background.

We see organizations who have taken many of these steps, but what typically holds them back from fully implementing them enterprise-wide are technology limitations. As a result, we see even very large global companies trying to manage this with spreadsheets. It's not that the technology solutions don't exist; it's the effort and cost required to deploy them that's holding many companies back.

The procurement function is increasingly being tapped to lead third-party risk efforts, given its role in engaging with external suppliers. At one global bank, the Chief Procurement Officer, reporting to the CFO, is leading a joint program of the procurement, risk, and legal organizations to manage and mitigate both internal and external third-party risk as part of a larger transformation of the bank's procurement and sourcing operations.

The project has several aims. Standing up a comprehensive program to meet U.S. and global regulatory expectations is one. A broader driver is to implement leading third-party practices that demonstrate the bank's ability to secure and protect its own resilience, thus contributing to the security and resilience of the global financial system at large. Given the interconnectedness of the global Financial Services industry; the location of bank offices, affiliates, and suppliers in various sovereignties; the frequent use of offshore resources in the course of financial transactions; and the current regulatory focus on Recovery and Resolution Planning in the wake of the financial downturn, the bank considers third-party risk management an imperative.

¹ See <http://www2.deloitte.com/us/en/pages/risk/articles/coso-enhances-internal-control.html>.

Learn more about identifying and mitigating third-party risk by contacting:



Kristian Park
kpark@deloitte.co.uk



Kristina Davis
kbdavis@deloitte.com



Walter Hoogmoed
whoogmoed@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 210,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Share this Risk Angle

