Deloitte.

Risk Angles
Third-Party Risk

This edition of Risk Angles looks at third-party risk and how organisations are managing third parties to address the inherent risks. Then, we take a closer look at how companies are approaching third-party risk identification, assessment, and mitigation, helping organisations be in control.

Simply put, third-party risk is the potential risk that arises from organisation's relying upon outside parties to perform services or activities on their behalf. 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 organisations are managing third parties to address the inherent risks. This paper discusses the escalation in third-party risk and the ways organisations should be mitigating it - but often aren't.

Third-Party Risk

Question	Deloitte point of view
The challenge **Why is third-party risk escalating?**	A few factors are in play. First, volume. During the recession, we saw many organisations 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 rands. 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 organisations 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 organisations, it's rare for someone in the organisation 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. In other instances, the legal function assumes they have third-party risks covered, but appear to have this false sense of comfort because their bias is towards ensuring good contracts rather than monitoring the implementation of these contracts.

Question	Deloitte point of view
The impact **What's been the traditional approach to managing third-party risk and where is there room for improvement?**	Third-party risk has typically been addressed in a siloed fashion, with individuals in the organisation 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 organisations 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 organisation have differing perspectives. For example, Chief Procurement Officers will often say 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 **What are leading companies doing to manage third-party risk?**	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. Data protection regulation identifies this as a privacy impact assessment and must be carried out on all high risk third parties. 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 organisation with a risk management background. We see organisations who have taken many of these steps, but what typically holds them back from fully implementing them enterprise-wide are technology limitations and a lack of centralised resources and artefacts. 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. Most organisations are unable to source the actual agreements with third parties.

A closer look: Examining the extended enterprise

Over the past two years, adoption of the 2013 COSO Internal Control – Integrated framework[1] 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

[1] http://www2.deloitte.com/us/en/pages/risk/articles/coso-enhances-internal-control.html

2015 we are starting to see the focus shift to operations and compliance due to the inception of further regulation that has an impact on third party service providers.

In that time, concern about third-party risk has risen much higher in many organisations. Senior leaders and boards have recognised 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 organisations 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 organisation. Inter-affiliate service providers are increasingly a focus of regulators, particularly those that supervise entitles outside the country of the parent. However, the ever changing regulatory environment that provides regulation around data protection and outsourcing has attracted regulators’ attention to third party risk from a legal and reputational perspective. 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. From a South African perspective, the South African Reserve Bank has brought forth a paper that establishes outsourcing requirements for financial institutions.

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 organisations 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. This has become a common trend in the application of regulations that do not merely affect one area of a business such as data protection.

The project has several aims. Setting up a comprehensive program to meet 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 financial system at large. Given the interconnectedness of the Financial Services industry; the location of bank offices, affiliates, and suppliers; 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.

There is an obvious upside in addition to safe-guarding the entity’s value – proper management of third-party risks often increases the entity’s ability to identify synergies, renegotiate more beneficial arrangements and leverage optimisation opportunities.

For more information, contact:

Navin Sing
Managing Director: Risk Advisory Africa
Tel: +27 31 560 7307
Email: navising@deloitte.co.za

Dean Chivers
Africa Leader: Risk Advisory Governance, Regulatory & Risk
(Johannesburg)
Tel: +27 11 806 5159
Email: dechivers@deloitte.co.za

Nina le Riche
Director: Risk Advisory
(Cape Town)
Tel: +27 21 427 5669
Email: nleriche@deloitte.co.za

Zama Dlamini
Director: Risk Advisory
(Durban)
Tel: +27 31 560 7177
Email: zamdlamini@deloitte.co.za

Igna Gray
Director: Risk Advisory
(Pretoria)
Tel: +27 12 482 0096
Email: igray@deloitte.co.za

Sisa Ntlango
Director: Risk Advisory
(East London)
Tel: +27 43 783 4006
Email: sntlango@deloitte.co.za

Munier Damon
Director: Risk Advisory
(Botswana and Namibia)
Tel: +27 21 427 5657
Email: mdamon@deloitte.co.za

Graham Dawes
Director: Risk Advisory East Africa, West Africa and Central Africa
(Nairobi)
Tel: +254 71 989 2209
Email: gdawes@deloitte.co.za