Deloitte.

Third-party challenges
Adding value by minimizing associated third-party risks

The emerging strategic perspective, together with the severity of the consequences of third-party-related incidents, is compelling organizations to catch up swiftly on upgrading the maturity of their third-party governance and risk management (TPGRM) processes – in order to create, as well as protect, organizational value. And although third-party risk has started featuring consistently on Board agendas, the supporting tools, technology, and processes are largely incapable of achieving the intended results. As the demands of TPGRM keep increasing, the majority of organizations are investing in centralized in-house functions to support the management of third-party risk. However, a significant proportion of organizations remain undecided on this matter, due to lack of understanding of their third-party ecosystem, together with inadequate knowledge of the marketplace for external providers. Deloitte can accompany you on the way to solving these and other challenges.

Organizational focus on third-party risk has traditionally been reactive and dependent upon who is driving the activity. Such a decentralized approach to risk has led to micro-focus on risk areas that interest certain parts of a business or certain functions (for example, operational performance from a supply chain perspective or information security from a corporate security angle). Organizations are only now starting to depart from this siloed approach and take a Board and leadership-led holistic, proactive approach to risk as a source of organizational value. This covers all categories of third parties and all areas of risk, considering operational risk factors (e.g. performance, quality standards, delivery times, KPI/SLA measurement), reputational/financial risk factors (e.g. labor practices, an understanding of financial health, appropriate charging mechanisms, and adherence to these) and legal/regulatory risks (e.g. compliance with bribery regulations, awareness of global industry standards as they apply to third parties, Environment and Health & Safety compliance).

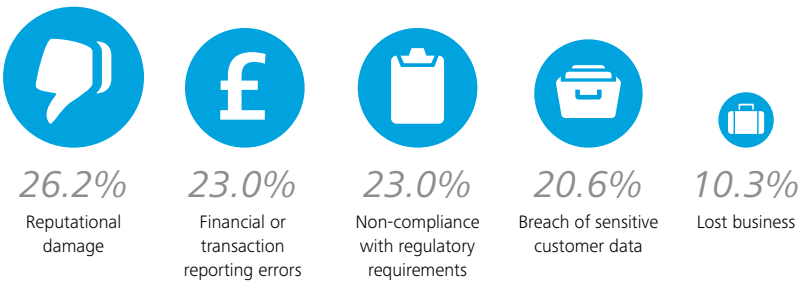
Deloitte believes those organizations that have a good understanding of their third-party business partners can not only avoid punitive costs and reputational damage, but stand to gain a competitive advantage over their peers, outperforming them by an additional 4-5% ROE (which, in the case of Fortune 500 or FT500 companies can mean additional EBITDA in the range of EUR 20–500 million). Academic researchers concur with this view. When stakeholders are able to appreciate improvements in governance, controls, and risk management that enhance their long-term expectations, equity values will rise.

Managing third-party risk

As incidents relating to third parties continue to rise, organizations are becoming more and more concerned about any resulting disruption to customer service or violations of regulations, given the growing severity of the related punitive action by regulators and customers. At the same time, increasing decentralization of operating units is starting to create challenges to a unified and consistent approach to Third-Party Governance and Risk Management (TPGRM). This trend drives organizations to mandate consistent third-party management standards across their operating units, aspiring to increase their monitoring and assurance activities over third parties.

The failure of large multinational businesses to appropriately identify and manage third parties can lead to fines and direct compensation costs or other revenue losses in the range of EUR 2–50 million, while action under global legislation such as the US FCPA can be far higher, touching EUR 0.5–1 billion. This point of view resonates with academic research, which has established that punishment by regulators causes losses to shareholders that are, on average, 10 times the size of the fine itself and negatively impacts share prices by an average of 2.55% in the three days after the announcement in which direct harm to customers and investors is involved. This of course is in addition to the significant reputational damage that an organization will suffer.

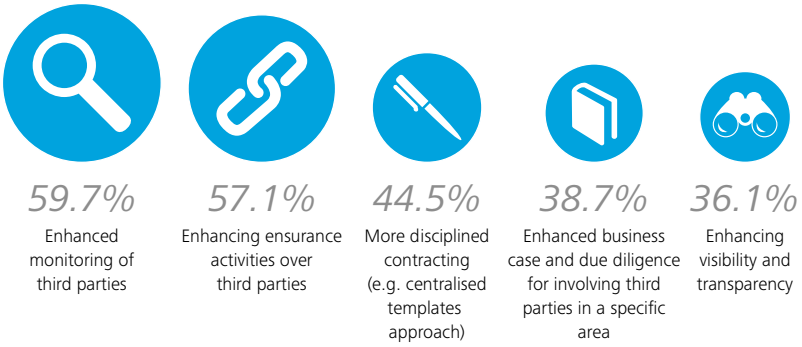
Fig. 1 – Impact of third party incidents actually faced by global survey respondents[1]



[1] The Deloitte 2016 global survey on Third Party Governance and Risk Management is the second in a series of publications on this topic, providing the results from over 170 organizations on the key issues and trends impacting their approaches to managing and mitigating third party risk.

The organizational demand for increasing monitoring and assurance-related activities around third parties demonstrates growing awareness that implementing controls to manage third-party risks is not a one-off activity. Given the dynamism in the external environment as well as within their extended enterprise, organizations must continually ensure that changing conditions have not made these controls out-of-date. In addition, more and more organizations appreciate the need to continually evaluate the effectiveness of these controls to reconfirm that they are working effectively, using various monitoring mechanisms.

Fig. 2 – Risk reduction initiatives taken up by global survey respondents



However, the lack of organizational confidence in the tools and technology used for third-party management results in the absence of reliable data in this area and thus reinforces the need for "other organizational assurance mechanisms" to obtain comfort on third-party management.

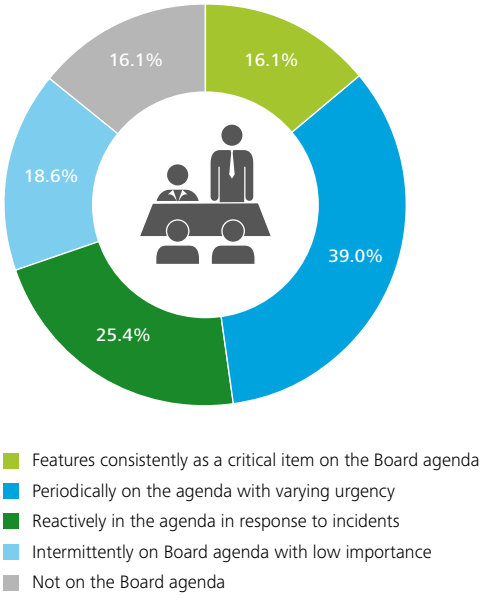
Third-party governance

It is encouraging to see third-party risk starting to feature consistently on the Board's agenda in the more forward-looking organizations, supported by increasing awareness and commitment to this issue. However, the Deloitte 2016 Global Survey reveals a wide implementation gap resulting from the inability of supporting tools, technology, and processes to achieve the intended results, despite commitment and a high-level governance framework being in place. Specifically, 94,3% of respondents have only low to moderate levels of confidence in the tools and technology used to manage third-party risk and 88.6% have a similar level of confidence in the quality of the underlying risk management processes, despite significantly higher levels of confidence in commitment and governance frameworks – thus creating an implementation gap.

At the same time, the organizational acceptance of the need for enhanced accountability for third-party risk management at the Board and C-suite levels is growing. Thus the explicit linkage of risk and strategy can be used to maximize the opportunities arising from third-party ecosystems. In the aftermath of the financial crisis, key regulators/governance bodies now agree on the Board's central role in approving and monitoring strategy, in keeping with their fiduciary duties to shareholders. The Board therefore needs to understand the risks and ensure appropriate risk management, which would further enable them to achieve a better balance between risk supervision, growth, performance, and strategy.

Deloitte experience in the area of TPGRM indicates that the growing complexity of third-party risks requires a holistic and deep understanding across a diverse group of organizational stakeholders, as well as disparate groups of third parties in the extended enterprise. This results in the utilization of a combination of methods for gaining assurance over third-party management, contributing to a balance between efficiency and effectiveness.

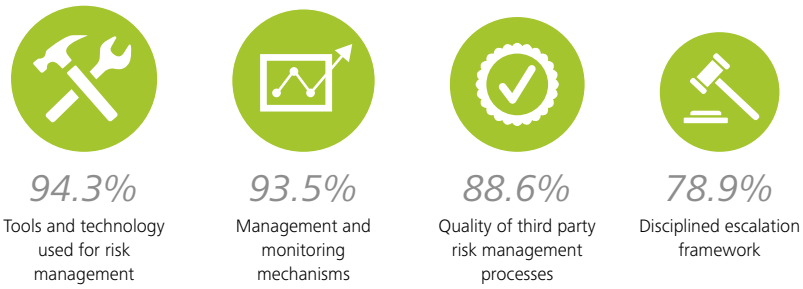
Fig. 3 – Third party risk on Board agenda (% of respondents)



Technology and delivery models

As the demands of TPGRM keep increasing, the majority of organizations are investing in centralized in-house functions to support the management of third-party risk, with a smaller proportion of organizations moving towards external service provider-based models. A significant minority remains undecided on their future course of action. There is no doubt that the lower level of organizational confidence in the tools and technology for TPGRM creates a burning platform to be addressed with urgency. The inadequacy of tools and technology reduces the effectiveness of reliable and timely data, adversely impacting the ability to make appropriate risk-informed decisions, as well as being able to implement optimized processes tailored to the type of product or service being outsourced. Deloitte experience indicates that appropriate tools and technology can signifi-cantly reduce pre-contract, post-contract and ongoing tracking/monitoring activities, thus resulting in available time for risk management personnel to complete their third-party risk management activities in a timely and effective manner.

Fig. 4 – Domains of third party risk management where confidence is moderate to low



The choice between a centralized in-house model for TPGRM versus an external service provider-based model is a vital decision that can have far-reaching strategic consequences, which need to be carefully considered and not undertaken recklessly. Deloitte believes that organizations moving to a centralized in-house function in this regard are primarily driven by the need to retain organizational control over this critical activity. This is enhanced by a better organizational understanding as well as the ability to manage a diverse group of stakeholders that an external provider may be unable to match. Deloitte experience further indicates that a lack of understanding of their third-party ecosystem, together with inadequate knowledge of the marketplace of external providers, may be resulting in a significant proportion of organizations remaining undecided in this matter.

"I think Deloitte's ability to coordinate global resources has been a huge benefit to us. As we have expanded worldwide, they have been able to meet our needs in every country we have moved to."

Client comment

Finding the right support

Deloitte has made significant investment and established a demonstrated, scalable, and cost-effective delivery model, which includes a dedicated project management office, global and local in-country teams for performing on-demand assessments, using various tools and accelerators.

Deloitte's risk-tiering methodology can help organizations to consider various risk drivers (e.g., the nature of information shared with a third party) and identify high-risk third parties. Inherent risk (or the entire risk-tier) is then used to define the frequency and rigor of risk assessments to be performed on a third party. Deloitte can complete remote and on-site assessments of your third parties and help you identify, for example, information security, business continuity, and/or legal or compliance risks. On issue of the third-party risk assessment report, Deloitte can coordinate directly with your third parties to develop and prioritize remediation plans, as well as to track remediation activities against target completion dates. Quality reviews are performed prior to the submission of assessment reports to confirm consistency.

Moreover, Deloitte can support ongoing monitoring requirements to continually assess your risk exposure to a third party – upon completion of the remediation activities, third-party processes, and/or controls are re-assessed to validate effectiveness and compliance with security requirements. Deloitte will provide executive and operational reports, based on an analysis of completed assessments (e.g., key themes, high-risk suppliers) and current review schedules (e.g., upcoming/completed assessments), in order to enable effective third-party risk management decisionmaking.

Face the challenge. Make the most out of it – with the best partner at your side

Your contact

Jan Minartz
Tel: +49 (0)40 32080 4915
jminartz@deloitte.de

For more information please visit our website www.deloitte.com/de

Issued 4/2016