KPMG

Is your provider secure?

Effective Third-Party Governance

For all firms that outsource their IT to third-party vendors or cloud providers, cyber security assurance remains a challenging area that lacks investment and focus. Businesses have increasingly been turning to third-party vendors for the provision of some or all IT and operational services. The use of third parties, although beneficial, can also expose an organization to increased business, security, intellectual property and structural risks that must be managed. Only when these risks have been identified and adequately managed, the true cost of outsourcing can be understood and the value of these relationships can be measured. The costs of not doing so could be dramatic – from regulatory fines and disrupted services to loss of customers and sales.

What's at risk?

All information related to your business carries value. Third parties that support you in key day-to-day and strategic areas of your business may handle or process various forms of information.

Information with recognized value
Intellectual property
Business processes
Customer, supplier and personnel data

Competitive advantage
Financials
New products
Business plans
New markets

Corporate transactions
Raising finance
Joint ventures
M&A
Divestitures

Vital business processes
Production
Financial
Retail
Safety critica

Understanding the value of information is core to understanding risk and the levels of controls required.

What are the drivers for change?

Industry leaders are now starting to centralize and professionalize the different methods in place in order to collect information from their suppliers and operate cyclical assurance and audit processes to assess their compliance. A number of key motives and drivers are behind this:

New technologies: Many organizations are following cloud-based and digital IT strategies. The widespread adoption of such disruptive technologies will raise the risk profile associated with third parties to acute levels.

Customer channels: New online and mobile channels, social media and web-based interactive systems will increase organizational exposure to potential liabilities in the event of a security breach.

Risk management: Organizations will need to formalize their activities and implement clear owners of third-party risk management that are responsible for the end-to-end process, from due diligence planning to remediation activities.

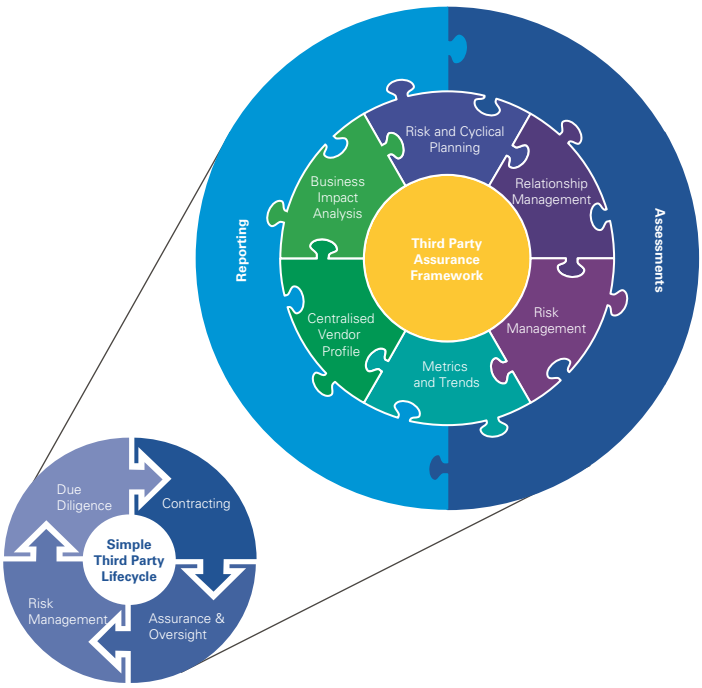
Regulatory focus: Fines and censure will become increasingly commonplace and new European legislation (e.g. GDPR) will further drive the regulatory compliance pressure. In the US, the regulatory focus on the protection of customer and business partner data will continue. The Consumer Financial Protection Bureau, the Wall Street Reform or the Consumer Protection Act prove this development.

Material risk warnings: The industry at large has started to acknowledge the issue. MELANI (2013/3) has issued material risk warnings around the lack of third-party oversight, particularly in the banking industry. This will continue to stimulate the need to act on third-party security risk.

Business partnerships: Business partners are demanding greater assurance over the supply chain. A number of business partners will issue third-party assurance activities a prerequisite of working together.

How we can help

KPMG has established a robust and scalable third-party governance framework and delivery model that enables you to put a secure third-party agreeement in place.



Our assurance framework covers all the key components required to run a centralized delivery and reporting service and can be deployed across all stages of the third-party lifecycle.

Activity	Description
Risk management	Oversight and assurance
Due diligence	Oversight and assurance
Contract	Contracts should be executed that minimize the risk of non-performance in line with the agreement.
Oversight and assurance	Vendors should be monitored and reviewed on an ongoing/regular basis to ensure continued delivery in line with agreed expectations.

We will work with you to identify the key elements of the third-party lifecycle that are most important to you, understand your supplier risk profiles, implement a framework for on-going assurance and undertake your risk based on third-party supplier reviews.

Benefits

- Our delivery model ensures that you have the right skills deployed at the right time, with the right levels of administrative support.
- By leveraging subject matter experts, we can mobilise quickly to provide a solution that's right for you.
- A risk-based approach ensures the greatest value from your budget and reduces your overall threat exposure.
- A defined methodology and consistent approach allows simplified stakeholder and third-party engagement.
- A flexible approach that adapts to and accommodates changes in legislation or the threat.
- Our understanding of a diverse range of third-party industries enables us to ensure the accuracy and completeness of our assurance reviews.
- Our reporting will allow you to understand trends and patterns across specific regions and business types.
- Our methodology can operate across multiple platforms or as a standalone process.

What sets us apart?

- We maintain a view of industry practice for real-time benchmarking.
- We deliver supplier reviews in more than 20 countries.
- We are not tied to any technology or software vendor. All our recommendations are independent and technical strategies are based solely on what is fit and appropriate for your business.
- We are able to leverage a Governance, Risk Management and Compliance (GRC) turnkey solution for the delivery of assessments and reporting.
- Our global presence enables cost-effective local delivery. KPMG is a global network of more than 152,000 professionals in 56 countries. We have more than 2,000 global security practitioners, giving us the ability to orchestrate and deliver to consistently high standards worldwide.

Contact

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

kpmg.ch

Thomas Bolliger
Partner, Information
Governance & Compliance
+41 58 249 28 13
tbolliger@kpmg.com

Matthias Bossardt
Partner,
Cyber Security
+41 58 249 36 98
mbossardt@kpmg.com

Gerben Schreurs
Partner,
Forensic
+41 58 249 48 29
gschreurs1@kpmg.com