Third Party Governance/ Cloud Compliance

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. The true cost of outsourcing can only be understood once these risks have been identified and adequately managed, thus allowing a proper measurement of the value of these relationships. 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 is of value. Third parties supporting you in key day-to-day and strategic areas of your business may handle or process various forms of information. Understanding the value of information is core to understanding risk and the levels of controls required.

What are the drivers for change?

Industry leaders have started 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. As a consequence, we expect that 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

Risk management processes are often ad-hoc. Organizations will need to formalize their activities and implement clear owners of third-party risks who are responsible for managing the end-to-end process, from due diligence planning to remedial activities.

Regulatory focus

Reprimands and fines will become increasingly common. Regulations such as the EU GDPR have reformed data protection and increased regulatory compliance pressure.

Materiality risk warnings

The industry at large has started to acknowledge the issue –the lack of third-party oversight. 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 to ensure that their interests are protected. Having numerous business partners will make third-party assurance activities a prerequisite for working together.

Clients' questions

Assessments and Audits

01	Requirements analysis – Are we aware of all of the regulatory and compliance requirements that need to be fulfilled by the third parties?	05	Service Provider Management – Is an internal governance with clear roles and responsibilities regarding third parties in place?
02	Transformation of provider requirements: How can the service provider transform regulatory and compliance requirements?	06	Cyber Security – Have we implemented adequate technical security measures to allow the outsourcing of our services?
03	Acceptance testing: How can we check that the service provider meets all of the requirements?	07	Controls, Risk Management and Auditability – Does our control framework also address outsourcing risks?
04	Service Level Agreement – Do our current SLAs cover all risks and regulatory requirements?	08	Compliance Management – Do our organization outsourcing services comply with the applicable regulatory requirements?

How we can help

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

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

We will work with you to

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

How we have successfully helped our clients

Client profile: A global technology company holding different types of data in data centers all over the world was planning to consolidate its data in regional data centers that were hosted by an external cloud provider.

Client need: KPMG was engaged to support the client's project by establishing an overview of the applicable regulatory requirements indicating the restrictions and mitigation measures when moving different types of data to various locations all over the world.

KPMGs approach: After having categorized the affected types of data, KPMG established – with the help of our experts from all over the world – an overview of regulatory requirements for different data locations all over the world, including the definition of mitigation measures.

Contact

KPMG AG
Räffelstrasse 28
PO Box
CH-8036 Zurich

kpmg.ch

Thomas Bolliger
Partner
Consulting

+41 58 249 28 13
tbolliger@kpmg.com

Robert Weniger
Director
Consulting

+41 58 249 70 19
rweniger@kpmg.com