Vendor security risk management

Cyber threats from vendors are increasing. Do you know your level of exposure?

The problem

KPMG recognizes that organizations don't have the capacity, investment support or skills to effectively manage the diverse number of suppliers found in today's large corporations. This results in:

- the potential for a large (or public) cyber security breach, attributed to the cyber practice failings of a vendor.
- lost value within commercial relationships (KPMG research estimates this can be up to 40%)
- increased risk exposure of supplier service failure or non- compliance, and
- failure to adhere to contractual obligations.

Compounding the problem is that not all supplier governance activities are continuous and therefore difficult to budget for and resource

How can we help?

KPMG's Risk Consulting practice provides services that help organizations identify and manage vendor risk management, designed to help protect your organization from a cyber attack due to a weakness of your third party.

KPMG has developed a suite of services to supplement the vendor security risk management function within organizations. This has the advantage of providing a cost effective, flexible service to:

- fill gaps in organisational skills sets
- provide specialised advisors who understand vendor security management
- match the demand and supply of supplier governance activities, and
- manage supplier risks by focussing on a wider set of suppliers based on their risk profile.

One off or irregular activities	Ad-hoc or point in time activities	Ongoing activities
– Vendor due diligence	– Delivery centre reviews – Cyber assessments – Supplier deep dive reviews	– Operational supplier management – Cyber assessments – Licence management

Source: KPMG in Canada

KPMG's vendor risk management approach

KPMG's Vendor Cyber due diligence is comprised of three specific areas of review and analysis:

- forensic background checks (company, management)
- cyber capability and adherence to good security practice, and
- dark-web reviews

KPMG is experienced at designing and implementing requirements of cyber security into third party contracts, and the ongoing process of assessment.

KPMG is also experienced at performing point in time, or cyclical cyber maturity assessments to assess the maturity of a third party's cyber program to address cyber as a business risk.

Typical deliverables

A vendor Cyber assessment will typically include on-boarding and scoping, stakeholder interviews, document review, evaluation against best practice and comprehensive reporting. We normally use our experienced panel of specialists to deep dive into your known and unknown risk areas.

Following on from this, we will provide an in-depth report showing our findings and your key Vendor related Cyber risks, based on our best practice framework and supplier risk maturity model.

Our report will typically contain recommendations to reduce your level of vendor Cyber.

Key benefits

By using KPMGs Vendor Security Risk Management services, key benefits typically include:

- adequacy and effectiveness of existing risk assessment processes from both your and your suppliers perspective; this typically includes interviews with selected suppliers;
- efficiency of operating model and alignment with good practice including assessment against KPMG's supplier risk maturity model;
- alignment of supplier risk to your risk appetite through policy and standard review:
- adequacy of your ongoing contract and SLA management, including reviews of current contracts;
- your approach to ongoing risk management, supplier risk reporting and management information from suppliers;
- a tailored and packaged service which addresses all of the major areas of vendor due diligence;
- leveraging of KPMG global network and market knowledge reach;
- the ability to embed activities as part of the annual vendor governance regime;
- reduction of risks introduced by third parties;
- ongoing governance of the cyber status of third parties;
- clear lines of communication and accountability for cyber requirements;
- more informed decisions through the use of information on measures, patterns of attack, and incidents; and
- a roadmap on vendor cyber risk management to increase cyber resilience.

KPMG's Cyber Team works with organizations to help prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

KPMG Cyber Security professionals believe cyber security should be about what you can do – not what you can't

An objective, knowledgeable advisor.

As a global network of regulated member firms, we have an unwavering commitment to precision, quality and objectivity in everything we do. So you can rest assured that KPMG cyber security assessments and recommendations are based on what's best for your business – not on market hype.

Knowledge of emerging issues.

In our I-4 Forum, also known as the International Integrity Institute, we convene leading cyber security professionals from around the world to discuss emerging threats, regulatory challenges and solutions. So we can help you consider possible issues around the corner in financial services, oil and gas, pharmaceuticals, engineering and other industries.

Rated no. 1 In executive management.

In fact, in a 2016 Forrester Wave™ study on information security consulting services, companies rated KPMG No. 1 for counseling senior leadership on cyber security. KPMG member firms surpass other professional services firms and technical firms to help board members understand cyber security, make informed decisions that align to the business strategy, and feel assured in their due diligence.

Transforming security across different geographies and cultures.

KPMG member firms have deep local knowledge in nearly every market where you do business, so we understand cyber security risks, regulatory impacts, change management, forensic investigations and other factors that may change from one country to the next. We have a global network of more than 3,000 cyber security professionals, plus multi-disciplinary collaboration with 189,000 other professionals in KPMG member firms across more than 152 countries. With that global presence, we can help you drive security transformation across your operations, wherever they may be.

Have a cyber emergency? Contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

Contact us

Francis Beaudoin
National Leader,
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

Jean-Francois Allard
Partner
T: 514 840 2645
E: jeanfrancoisallard@kpmg.ca

Yassir Bellout
Partner
T: 514-840-2546
E: ybellout@kpmg.ca

Erik Berg
Partner
T: 604-691-3245
E: erikberg@kpmg.ca

John Heaton
Partner
T: 416-476-2758
E: johnheaton@kpmg.ca

Adil Palsetia
Partner
T: 416-777-8958
E: apalsetia@kpmg.ca

Jeff Thomas
Partner
T: 403-691-8012
E: jwthomas@kpmg.ca