Security strategy & program development

Ensuring an effective cyber strategy is crucial for effective cyber risk management. Are you confident your cyber strategy is the right one?

The problem

KPMG recognizes that many organizations simply don't have the experience or capacity to appropriately define and develop the security strategy and program of the firm. This can create cyber weaknesses that can be exploited by malicious individuals. In addition, this can result in:

- the potential for a large (or public) cyber security breach.
- lost value within commercial relationships
- failure to adhere to contractual obligations.

In addition, it creates inefficiencies that can mean that the organization isn't getting the best '*bang for its buck*' when it comes to cyber spend.

Typically the security strategy and program development activities include the following key Phases:

- Phase 1: Kick-off, planning and project management;
- Phase 2: Identification of critical information assets;
- Phase 3: Cyber security risk/threat modelling and evaluation;
- Phase 4: Targeted maturity levels identification;
- Phase 5: Assessment of current security strategy, together with cyber security program adjustment and re-sequencing.
- Phase 6: Issuing the final report and presenting to management.

How can we help?

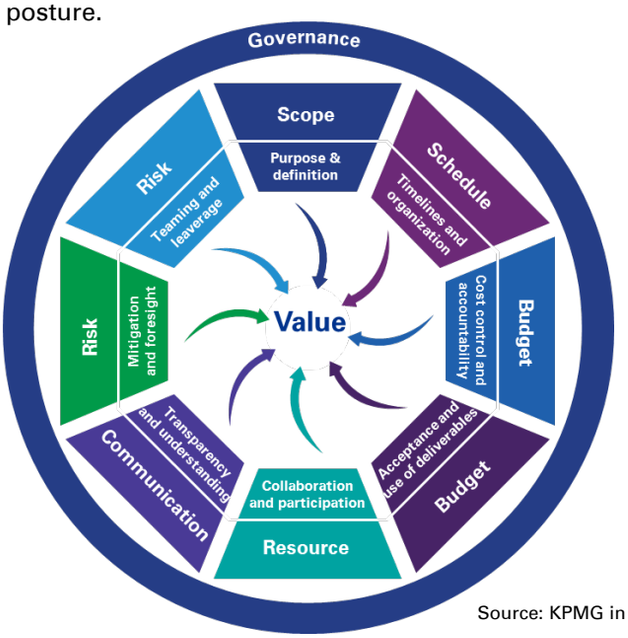
From strategy to implementation. No matter where you are on the cyber security journey, KPMG can help you reach the destination: a place of confidence that you can operate without crippling disruption from a cyber security event. Working shoulder-to-shoulder with you, KPMG professionals will help you define your organization's security strategies from the ground up, all the way through to completing reviews of existing plans.

KPMG 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's approach

KPMG will work with you to define a customized approach to help you with your strategy.

We take a phased approach by splitting the engagement into manageable work streams. We will spend time understanding the characteristics, capabilities, gaps and improvement opportunities for your cyber security posture.



Source: KPMG in Canada

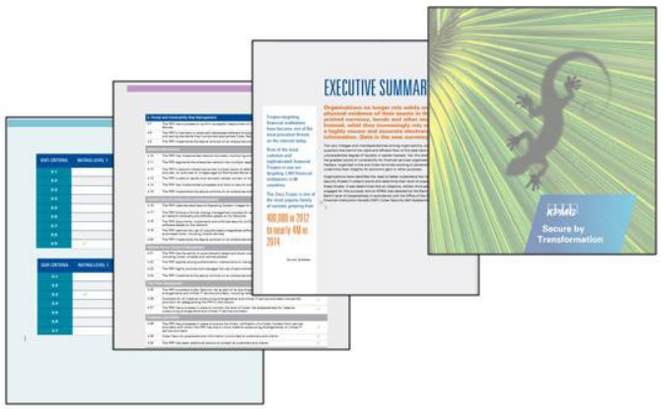
Our approach is to build on what is currently in place (if available), and provide the most appropriate cyber security strategy based on the most up-to-date information on cyber threats and risks.

The strategy will include a prioritized set of activities, and will include quick-win activities where appropriate. In addition, the strategy can take into account global considerations (for large multi-nationals) and provides appropriate Key Performance Indicators (KPI's) and Key Risk Indicators (KRIs) as metrics to track progress and provide updates to Boards and Executives.

Typical deliverables

Depending on your requirements, we will produce a clear, comprehensive report the provides effective sequencing for your security strategy and program development.

Depending on your requirements, we can provide approximate time-frames for activities, costing for each aspect of the strategy, time to complete each element, and can even make recommendations on who in your organisation would be best placed to be involved in each element.



Key benefits

KPMG's Vendor Security Risk Management services approach is as follows:

- Is based on a refined set of combined methodologies to conduct analysis and design, and assessment of business cases and strategies. Combined written materials and stakeholder engagement, allows us to rapidly engage, and to derive hypothesis and themes early in the engagement.
- KPMG professionals have deep knowledge of the current cyber threats and ways to mitigate risks and deliver capabilities. We will move into deeper assessment of capabilities and the operating model, involving stakeholders throughout the process.
- We will work with your teams in a highly effective and efficient way.
- Following the assessments, you will be provided with clear recommendations on approaches to help move towards a more effective security strategy, allowing you to make informed decisions on your future cyber plans and investments.
- The final report will contain a high-level executive summary, as well as details of our findings to support our analysis

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 counselling 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