Cyber resilience

Cyber threats are varied and are now able to affect any organization, in any sector at any time. Having effective cyber resilience and being prepared for a cyber incident places you in a stronger position to survive it.

Being ready – No matter what

Information availability is essential in the Information Age. Natural disasters, malicious intent, and catastrophic accidents can disrupt information availability and negatively impact key business processes. Moreover, competitive pressures and market demands, together with an increased dependence on technology for core business processes, are redefining the need for effective and risk-based cyber maturity. KPMG's cyber resilience service is a structured response to a disruptive or catastrophic event.

Being prepared for a disaster means your business is far more likely to survive, and reduce the impact of an event.

How can we help?

KPMG's Risk Consulting practice provides services that help organizations identify and manage cyber disruption events and reduce their vulnerability to a wide range of potentially devastating events.

These cyber resilience services cover the broad spectrum of the continuity/contingency planning discipline. The overriding goal is to help an organization resume critical operations within an acceptable time frame following an interruption.

Below is a list of the Cyber resilience services that we offer:

- development and/or assessment of Business Continuity Management program (policies, procedures, maintenance programs),
- business impact analysis,
- cyber threat and vulnerabilities assessments,
- business continuity planning,
- facilities and departmental plan assessments,
- third party service provider assessments and cyber resilience compliance reviews,
- disaster recovery planning documentation assistance and evaluations,
- test exercising assistance,
- crisis management plan development,
- emergency management plan development,
- employee notification protocol implementation assistance and assessments,
- incident reporting including command and control protocols, and
- development and/or assessment of senior executive and program monitoring activities.

KPMG's cyber resilience advisory service business continuity planning

BCP addresses major disruptions (natural or man-made) that impact the effective execution of an organization's core processes. All critical business areas and support functions are included in the planning process. KPMG has developed a flexible, modular approach that measures disruption risk, plan development, and plan refinement through periodic testing.

Disaster recovery planning

The disaster recovery planning (DRP) project focuses on the timely restoration of information technology (IT) support functions, shared computer systems, and voice and data communications. DRP assistance may be needed because an existing plan has become obsolete, or to help with the implementation of new systems.

Our approach

KPMG brings a business context to cyber security for all levels of the organization – from the boardroom to the back office:

- cyber security: It's a business issue, not just an information technology issue,

– translating cyber security into a language your business can understand,

– a business-led approach, supported by deep technical skills,

– working shoulder-to-shoulder as your approachable, attentive, strategic advisor, and

– KPMG has expertise in your industry.

We customize our approach to suit our client's needs. Critical success factors for these engagements include:

– The depth of experience we bring to our advisory services

– Our ability to team with management, implementation professionals, and internal audit personnel

– Our modular and easy-to-use methodology

KPMG's approach

We have a Three-Phased BCP Approach that can be customized to fit your organization's needs.

Phase I: Manage the risk

Phase II: Create the plan

Phase III: Test and administer the plan

Our approach helps ensure minimal disturbance of in-house resources and encourages the support and confidence of senior management.

Phase I: Manage the risk

Business Impact Analysis

A cyber business impact analysis (BIA) determines the potential impact of a disruption to the business. The BIA can range from a high-level qualitative estimate to a detailed analysis of tangible and intangible impacts on the business. Critical business functions are identified and prioritized, and the impact of shutting them down is estimated over time.

Risk and vulnerability analysis

A Cyber risk and vulnerability analysis provides an independent analysis of exposure to potentially disruptive events. Areas of investigation include physical exposures, existing protective measures, and cost/benefit/exposure reduction analysis.

Phase II: Create the plan

BCP and DRP

Continuity plans need to be created as well as updated to reflect new infrastructures, systems, processes, and other changes within an organization. KPMG can assist clients in expeditiously assessing the risk, formulating a mitigation strategy, and creating or updating the BCP or DRP. Specific threats (e.g., the presence of hazardous materials, potential adverse impact on the public, or special business characteristics) warrant special attention. KPMG helps clients develop highly focused planning, crisis response procedures, and business recovery actions.

Phase III: Test and administer the plan

Test Facilitation and Training

Test facilitation offers assistance with testing of existing Cyber plans either on a recurring basis or as requested. Services include guidance and assistance with test scenarios, test monitoring, and the evaluation of test results. Additionally, KPMG provides assistance in conducting orientation and training sessions.

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.

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

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

Have a cyber emergency? Contact our 24/7 Cyber response hotline at 1(844)-KPMG-911 (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

kpmg.ca/cyber