Cyber resilience

Empowering organizations to anticipate, adapt, withstand and recover from cyber threats.

96% of CEOs consider cybersecurity to be fundamental to business growth and stability, and 74% stress their concerns about organizational preparedness to reduce damage in case of cyberattacks.

Source: SentinelOne Cyber Resilience, 2025

Despite the greater due diligence of suppliers, 43% of organizations experienced supply chain disruption due to third party failures.

Source: BCI Supply Chain Resilience Report 2024

Why cyber resilience matters?

Disruptions are inevitable. From natural disasters and power outages to system failures and sophisticated phishing or deepfake attacks, these events can disrupt critical business operations. Cyber resilience helps you protect and sustain what matters most by making your organization stronger, more adaptable, and prepared to withstand and recover from these challenges. It's about ensuring business continuity and agility, even in the face of cyber incidents.

Why do you need it?

In today's digital landscape, cyber threats are more sophisticated, frequent and disruptive than ever. Organizations must not only defend against attacks but also ensure rapid recovery to keep operations running under pressure. Unlike traditional cybersecurity which focuses on preventing breaches, cyber resilience assumes breaches will happen and prioritizes continuity and adaptability. As a core element of operational resilience—including business continuity, crisis management, and risk management—cyber resilience integrates technical defences, strong governance, and a security-aware culture. This holistic approach strengthens your organization at every level, helping you withstand and recover from any cyber incident.

Cyber Resilience Model

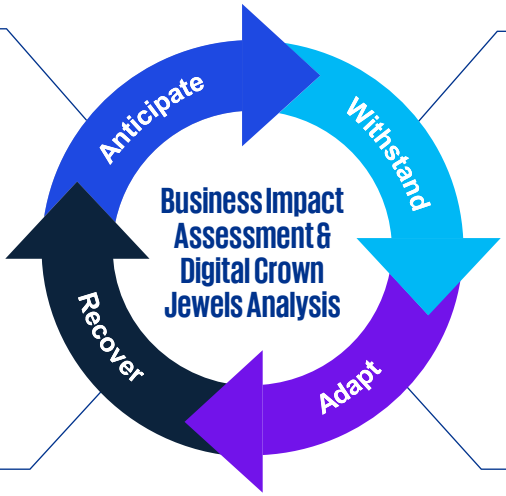
KPMG's Cyber Resilience Model outlines key areas that enable organizations to maintain mission-critical and business objectives even in highly contested cyber environments. At the core of this model are the Business Impact Assessment (BIA) and Digital Crown Jewels (DCJ) Analysis used to guide organizations to prioritize what matters most and continuously strengthen resilience practices.

Anticipate

Proactively assess the cyber threat landscape, perform risk assessments, and train users to identify and prepare for potential threats before they occur.

Recover

Restore operations efficiently by leveraging established incident response plans, validated through regular simulations and supported by robust backup strategies.



Withstand

Design systems and networks with resiliency in mind, using coordinated protection and processes to defend against attacks and keep operations running.

Adapt

Implement dynamic reconfiguration and redundancy to enable organization to quickly adjust systems, user privileges, and processes in response to evolving threats.

Our cyber resilience service offerings

We provide a range of services that help organizations stay strong and keep running, even when faced with cyber challenges. Our approach focuses on four key areas: anticipate, withstand, adapt, and recover. While our dedicated Cyber Resilience team leads these efforts, we also bring in specialists from other areas when needed to ensure every solution fits within our proven Cyber Resilience Model.

Board-level and executive education

We deliver tailored briefings and sessions for boards and senior leadership, focusing on cyber risk governance, regulatory expectations, and strategic resilience planning. These sessions empower executives to make informed decisions, fulfill oversight responsibilities, and strengthen organizational resilience from the top down.

Cyber Resilience planning

We support the development of resilience documentation and organizational enhancements, including Digital Crown Jewel Analysis, Disaster Recovery Plans, Business Continuity Plans, Specified Resilience Plans, and Incident Response Playbooks. Our approach ensures these plans are practical, tested, and aligned with your business priorities.

Cyber resilience maturity assessment

Using KPMG's Cyber Resilience Framework, we provide comprehensive, tailored assessments through a unified, scalable, and repeatable approach. This framework aligns with industry standards and regulatory requirements, offers benchmarking, and helps organizations navigate uncertainty. The result leads to actionable insights and practical recommendations to reduce risk and strengthen resilience.

Security awareness training

We deliver targeted security awareness and training services, leveraging next gen AI-powered platforms that help employees recognize and respond to common cyber threat vectors, such as phishing, smishing, and deepfakes. This training equips end users with practical skills to identify suspicious activity, avoid falling victim to attacks, and report incidents promptly.

Tabletop exercises (TTX)

We design and facilitate customized tabletop exercises and simulation workshops to build organizational readiness for cyber incidents. These interactive sessions engage specific teams or cross-functional groups—including executives and technical staff—to test response protocols, improve decision-making under pressure, and develop muscle memory for real-world scenarios. KPMG offers flexible delivery formats to fit your organization's needs—virtual-only, in-person, or a hybrid—enhanced with advanced tools such as our 4Di simulator for increased realism and effectiveness.

What makes KPMG different?

KPMG in Canada brings together cyber resilience and information security professionals across the country – from Vancouver to Halifax – supported by global expertise. We think globally, act locally, and deliver deep industry knowledge to help you focus on what matters most: protecting your critical assets and ensuring a cyber resilient posture.

Leading methodologies

We go beyond industry frameworks by leveraging and continuously enhancing KPMG's Cyber Resilience Framework. Our approach expands on emerging regulatory practices to deliver comprehensive assessments and grounded direction, ensuring your organization is measured holistically.

Focused on collaboration

With 300+ resilience professionals across Canada, we focus on delivering better resilience capabilities. We work hand in hand with your team and collaborate with our Cyber Threat Intelligence and Incident Response practices and other specialists to deliver actionable insights that strengthen your organization.

Proven commitment

Our relationships are built on trust and long-term partnership, delivering effective and efficient solutions that evolve with your business needs. We are deeply invested in your success, just as we have been in Canada since 1869. As part of the KPMG's global network, we combine worldwide expertise with local insight to help you focus on what matters most.

Contact us

Vivek Jassal
Partner
KPMG in Canada
416-777-3723
vjassal@kpmg.ca

Tarek Habib
Partner
KPMG in Canada
902-292-2091
tarekhabib@kpmg.ca

Ivana Lukic-Miloloza
Senior Manager
KPMG in Canada
416-777-8545
ilukic-miloloza@kpmg.ca