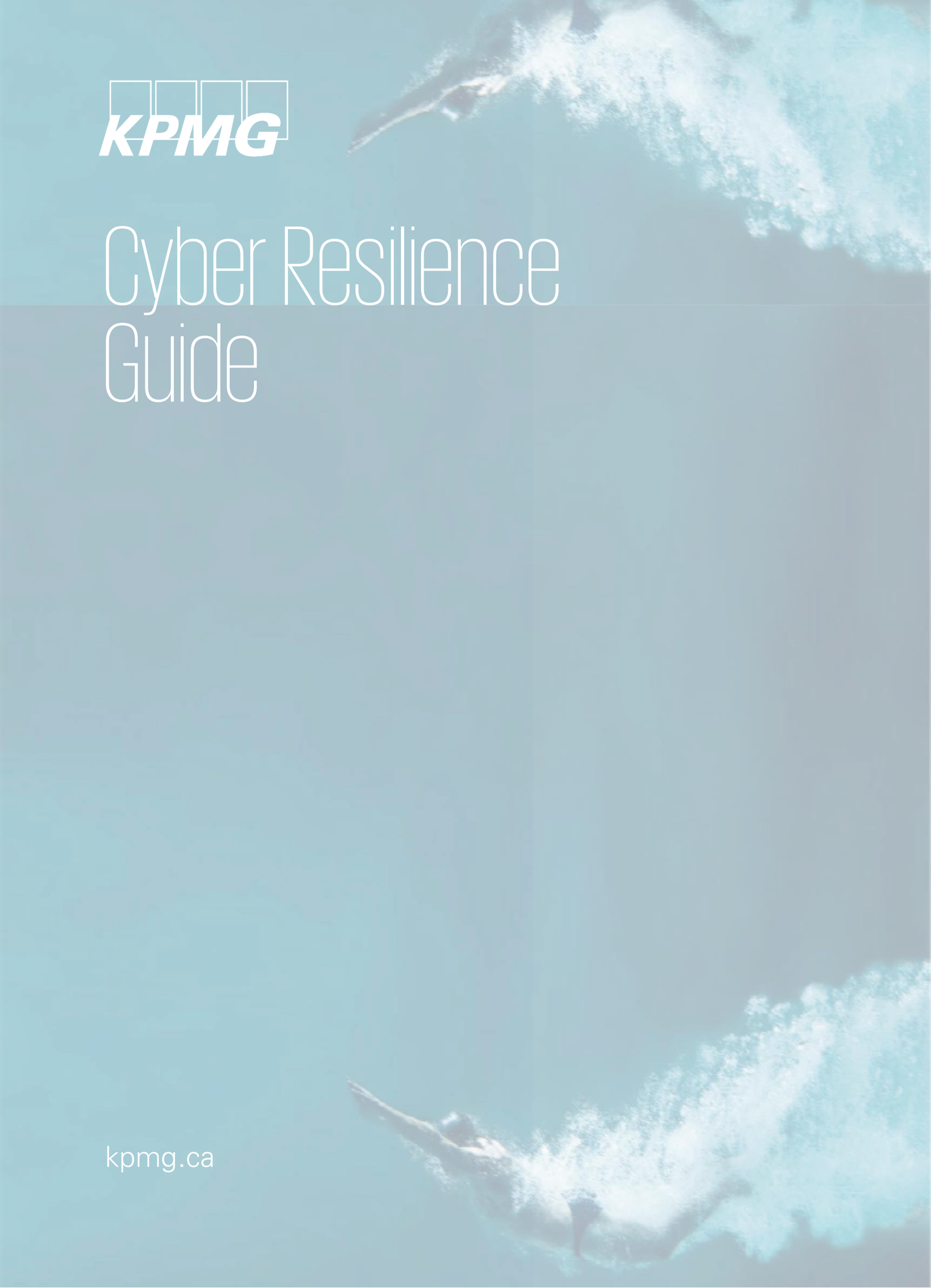
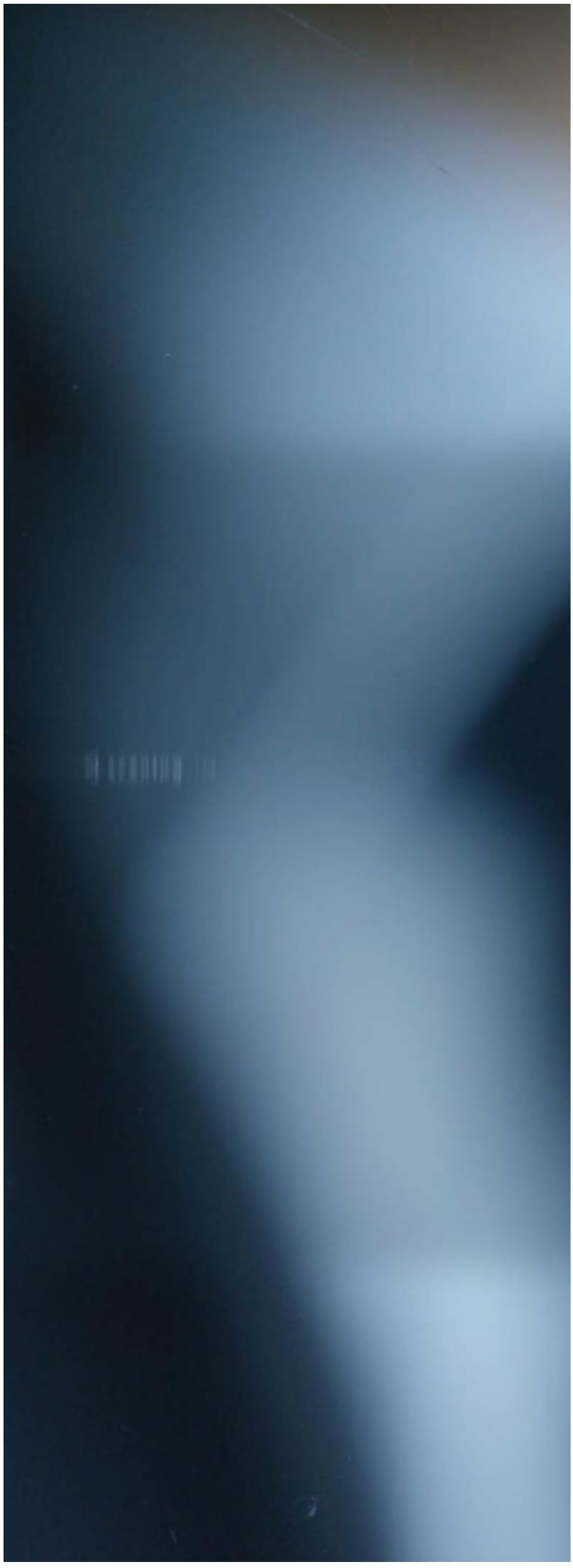


Cyber Resilience Guide

kpmg.ca



Contents

Introduction

"Organizations' resilience to cyber threats and the unimpeded, safe and secure flow of appropriate information and data [...] are critical to improving outcomes for all". This was one of the key messages of the Government's response to the National Data Guardian's review of Data Security.

In a global landscape of **increasing digital threat**, populated by sophisticated hackers and cyber criminals, the ability to **prepare** for, **respond** to, and **recover** from cyber attacks is more important than ever before. The cyber resilience service line is dedicated to developing and enhancing these vital capabilities, ensuring organizations can protect themselves against cyber risks, defend against and limit the severity of attacks, and ensure **continued survival in the aftermath of cyber crime**.

With traditional cyber security measures no longer enough to reliably protect organizations from persistent, high level attacks, resilience provides for **a safer, more reliable digital business environment**. This guide will go on to explain some of the key elements of cyber resilience that are relevant for technology-reliant businesses, and assist you in taking the necessary steps to improve your cyber environment.

KPMG can support your organization using the following framework:

Enterprise Recovery

The focus of Enterprise Recovery is in helping organizations recover from catastrophic cyber or technology failures. We use extended business impact assessments, business services assessment workshops, technical and architectural design assessments and questionnaires to collect critical service information in order to identify, prioritize and map critical applications and infrastructure.

Crisis Management Program

KPMG design and deliver a series of independent cyber security simulations to test an organization's cyber incident response, business and board crisis management procedures when faced with a cyber focused disruption scenario.

Business Continuity

KPMG design and deliver end-to-end business continuity, IT Disaster Recovery and resilience services, with targeted review and assessment of existing capabilities to provide a road-map for improvement.

USCR - Unified Security & Crisis ResilienceModel

KPMG have a proven track record in testing an organization's cyber defence from the perspective of an attacker, via active technical assessments. The vulnerabilities identified by our in-house incident response teams allows for a unique testing of an organization's crisis management teams.

What is Cyber Resilience?

Cyber resilience refers to an organization's ability to recover from a successful cyber attack with as little business disruption, regulatory conflict, and reputational impact aspossible.

A holistic approach to crisis, integrating human irregularity with technical considerations, defines KPMG's approach to resilience.

Our journey has included resilience work with some of the largest clients in the world, including major banks, energy companies, insurance companies, and multinational conglomerates. Backed up by this wealth of experience, KPMG is perfectly placed to **identify** cyber weakness, **evaluate** risk, and **mitigate** it, thereby improving immeasurably your security and longevity.

Why is it important for your business?

In a globally connected world of increasing digital threat, populated by sophisticated hackers and cyber criminals, the ability to **prepare for, respond to, and recover** from cyber-attacks is more important than ever before.

The days of an efficient, well-tested cyber security system making a successful cyber attack improbable are over. **Cyber breaches have become inevitable** for any technology-driven business.

Amidst **increased regulation** concerning data privacy, there are heavier financial implications than ever before to a serious breach. A rigorous cyber resilience procedure provides the final defense in a crisis, and may save an organization from an otherwise terminal cyber attack.

Today's challenges

01 There is an **inconsistent understanding** of cyber resilience across organizations especially among senior stakeholders.

02 Cyber Resilience is **rarely incorporated** into an organization's vision, values and business strategy.

03 Cyber Resilience is not often considered during the **decision making process**.

04 There exists minimal to no **incentives or drivers** around delivering Cyber Resilience.

05 There is a **lack of ownership and accountability** across business functions with regards to Cyber Resilience.

"KPMG handled a scope of work to prepare the firm from a PRA onsite review on Operational Risk and Resilience as part of their supervisory program. Our experience with KPMG was very positive with regard to our scope of work and KPMG exceeded our expectations."

John Coffrey – Chief Risk Officer, Ford Credit

"[KPMG are] consultants with operational experience who have deeper insights on the day-to-day battles clients fight than typical service delivery personnel with just a consulting background."

Forrester Wave™: Information Security Consulting Services, 2017, Forrester Research Inc. 2017

Enterprise Recovery

What is Enterprise Recovery?

Enterprise Recovery focuses on helping organizations **recover from catastrophic cyber or technology failures** through extended business impact assessments, business services assessment workshops, technical and architectural design assessments and questionnaires to collect **critical business service information.**

Why do you need it?

Cyber attacks have become a common occurrence and they are growing **more sophisticated** every day.

In the realm of **more complex business and technology integration**, organizations need to plan for severe but plausible disruptions in order to effectively recover and respond to disruptions.

Organizations need a **robust program and strategy** for recovering critical IT services and business operations in the event of catastrophic business failures.

Organizations need to quickly identify their **key critical services and applications** to respond and recover from crises.

Businesses need to ensure critical **customer-facing** business services are always **accessible and functional** when faced with a disruption.

Benefits of Enterprise Recovery

Aids in the **recovery** from catastrophic cyber and technology failures.

Identifies and **prioritizes critical applications** and infrastructure.

Improves **efficiency in the recovery** processes through the design of tailored solutions.

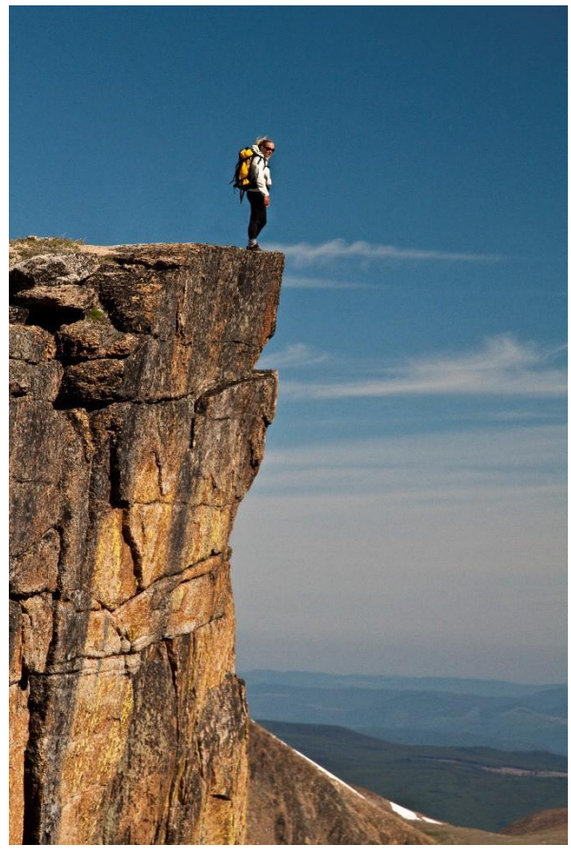
Builds confidence of an organization to work through their recovery processes in a crisis.

Empowers senior management to respond effectively to crisis situations.

Improve **communication plans** and documentation of processes.

How do we achieve this?

- **Critical Business Service Identification** uses extended business impact assessments, business services assessment workshops and questionnaires to identify, validate and prioritize your critical business services.
- **Key Dependency Mapping** identifies the dependencies that impact critical service infrastructure by mapping onto the five pillars: people, technology, data, property and third parties.
- **Strategic and architectural design of recovery solutions** helps you develop strategic and architectural designs focused on the recovery of critical business services.
- **Development of playbooks and plans for Enterprise Recovery** provides step by step instructions on how to work through the recovery of your organization. It incorporates aspects such as communication plans, escalation procedures and crisis recovery processes.
- **Simulations and testing of recovery solutions and IT** use severe but plausible scenarios to assess how well executives and senior management respond to crisis situations using the playbooks and documentation developed.



KPMG's Approach

Phase 0: Mobilization

- Identify the key stakeholders.
- Identify key workstreams that cover technology, process and governance, contractual & legal
- Request the relevant documentation.
- Development of overall program plan and leadership structure
- Development of project plans and leads
- Definition of project management capability e.g. standard or agile

Phase 1: Critical Business Service Mapping

- Understand your current maturity and identify any gaps in your recovery capability through the use of questionnaires.
- Develop a critical business service mapping methodology and required mapping templates.
- Hold multiple workshops to identify and validate your critical business services. This will help define the skeleton company as part of the recovery program.
- Identify and define impact tolerances and KPIs (such as Recovery Time Objective, Recovery Point Objective and Maximum Acceptable outage) for each business process and business service in scope.

Phase 2: Key Dependency Mapping

- Using the identified critical business services, we will hold multiple workshops to map key dependencies on the five pillars: people, technology, data, property and third parties.

Phase 3: Build & Develop

Phase 3A

- We will work with you to develop appropriate playbooks and runbooks to provide you with step by step instructions in order to work through your enterprise recovery process.
- The plans developed will incorporate aspects such as communication plans, escalation paths and recovery processes with a focus on the critical businesses identified in phase 1.

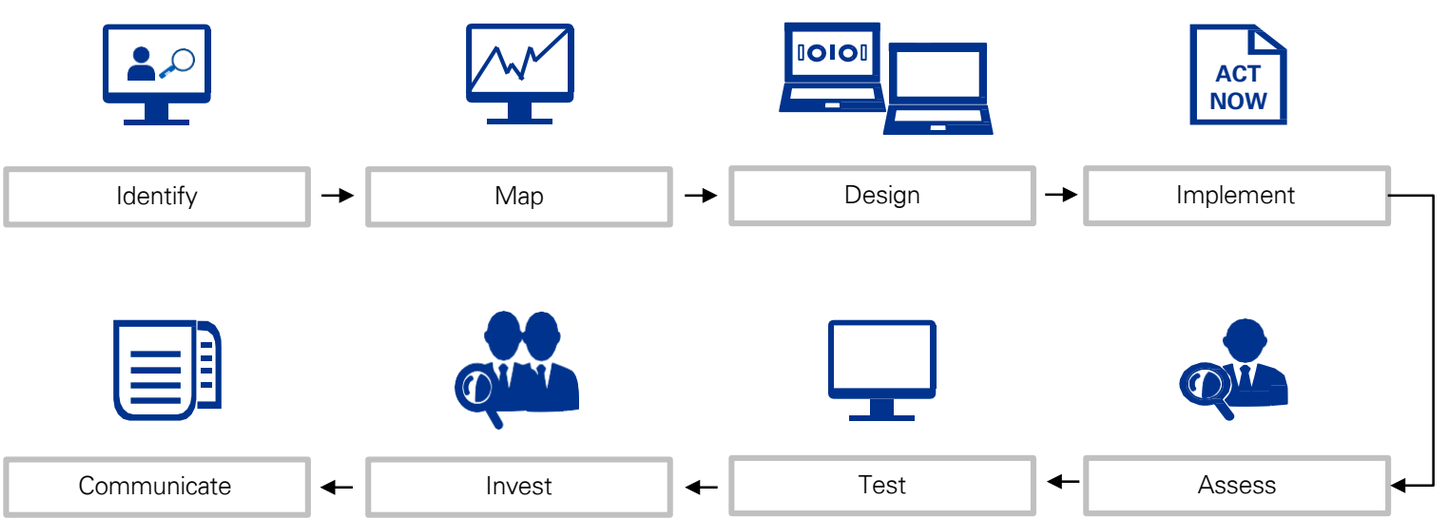
Phase 3B

- We will conduct an architectural design of the your live environment to include vaulting solutions.

Phase 4: Scenario & Stress Testing

- We will use severe but plausible scenarios to test the accuracy and effectiveness of impact tolerances and KPIs identified as part of phase 1.
- This phase will test the response capabilities of incident response teams as well as the effectiveness of the playbooks created as part of phase 3.

Key processes to Enterprise Recovery



Crisis Management Program

What is Crisis Management?

In an increasingly volatile business environment, organizations not only have to **prepare** for crises, but **expect** them. An organization's ability to not only detect incidents and crises as they occur, but **effectively respond to and recover from them** is increasingly under scrutiny.

An organization's crisis management framework (CMF) is the foundation which enables **escalation, communication** and **co-ordination** during a crisis. It also provides the structure through which to train and exercise stakeholders with crisis management responsibilities. Exercises leverage tailored risk-based scenarios designed to simulate the pressures on and expectations of individuals and the organization, during a crisis.

Developing a Crisis Management Program

A Crisis Management Program allows an organization to:

- Develop a series of **independent cyber security simulations** to test their cyber incident response, business and board crisis management procedures when faced with a cyber focused attack;
- Develop an exercising capability that includes a **governance structure** and related processes to periodically test their cyber incident response;
- Design fit for purpose **reporting mechanisms** for the business and the board.
- Test the response and recovery capabilities **across multiple business lines and geographies by** conducting several exercises over a number of predefined months

Benefits of a Crisis Management Program

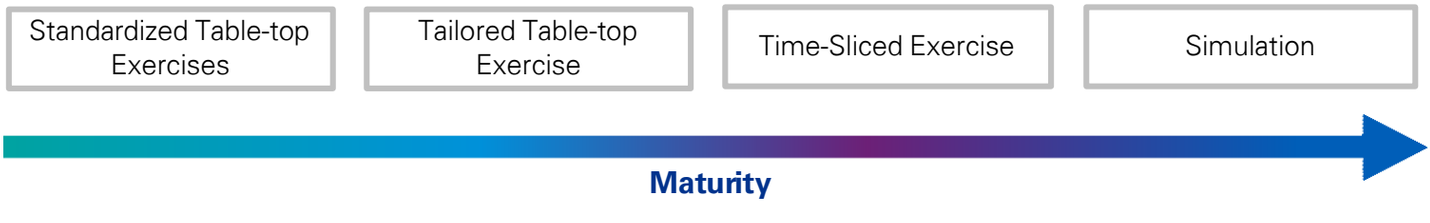
- Validate the effectiveness of response strategies in a **safe, simulated environment**
- **Build capability** amongst the individuals expected to respond to a crisis
- **Empower key stakeholders** to know when to act and how to act during a crisis
- Build **comfort** around how to respond to a number of different crises
- Improved **visibility of risks** and mitigating actions taking place
- **Identify gaps** in business processes before it is too late

Why do you need it?

- Without a thoroughly tested, coordinated response to cyber crisis, no organization can be confident in its future projections, given the nature of **operating as a business is increasingly fraught with cyberperil.**
- With a wide variety of available exercises, KPMG is perfectly placed not only to prepare an organization for the worst, but also to **ensure confidence amongst shareholders and employees** of sufficient preparation to mitigate the most serious regulatory penalties.
- Outcomes from a Crisis Management Program can be used as a guide to **future strategy development** to help **an organization protect themselves** against cyber risks, defend against and limit the severity of attacks, and ensure its continued survival despite a disruption to critical business processes.

Crisis Management Exercise Maturity

The appropriate exercise format is dependent on your maturity as shown below.



KPMG's Approach

Phase 0: Mobilisation

- Request relevant crisis management documentation e.g. Incident Response Plan
- Identify key stakeholders to support the development of the scenario. For example, a Programme Lead and various Subject Matter Experts.

Phase 1: Exercise Preparation

- Kick off meeting to agree the scope and objectives of the exercise.
- Understand processes in scope as well as associated vulnerabilities in the business area.
- Discuss initial scenario ideas.

Phase 2: Exercise Design

- Hold workshops with SME(s) to develop and agree final scenario.
- Produce a Master Events List (MEL) and injects to support scenario.
- Hold a Dry Run to finalise the MEL and injects created.
- Finalise attendees and logistics.

Phase 3: Exercise Delivery

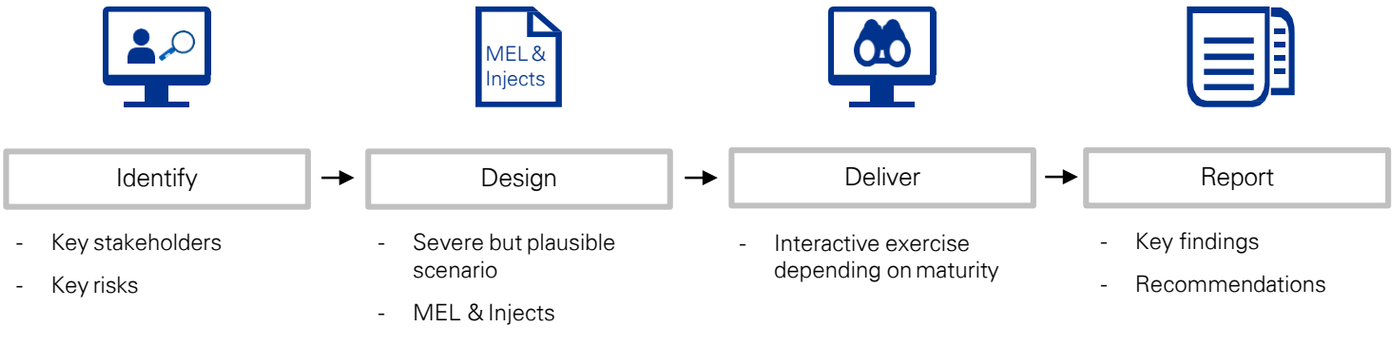
- KPMG to facilitate an interactive simulated exercise to test the required teams.
- Hold a hot debrief session to reflect on the participants performance.

Phase 4: Exercise Reporting

- Executive summary including high level remediation actions.
- Detailed report outlining strengths and weaknesses of response and recovery activities.
- Report results and findings to senior stakeholders.

The 4Di Simulator

- **Innovative and versatile solution** that enriches training environments to deliver immersive, challenging and realistic crisis management simulations.
- The **mobile platform operates on smart phones, tablets and laptops** and can be used anywhere with an internet connection globally, whether at the same site or multiple locations.
- **The tool** is used to **deliver injects, record all actions taken** and facilitate communications between teams.
- **Participants should record all decisions** made and courses of action taken into the tool to ensure their responses to the simulation can be thoroughly assessed.



Business Continuity

What is Business Continuity?

Business Continuity capabilities are an organization's ability to **protect and sustain critical business processes** during a disruption. Effective **business continuity management (BCM)** ensures that firms are equipped with the ability to prevent, respond to and recover from various operational disruptions.

Why do organizations need it?

Businesses may incur **significant costs** of not operating during a period of downtime. They can suffer not only **financial,** but **reputational** and **operational damage.** For example, loss, damage or denial of access to key IT services, may cause delays in key services an organization offers.

Organizations need a **robust program and strategy** for recovering critical IT services and business operations in the event of catastrophic business failures.

Organizations that are resilient are better able to withstand shocks, **protect shareholder value** and navigate disruptive change.

We help organizations **prevent, detect, withstand and respond** to incidents that threaten to compromise the safety of their staff or the continuity of their critical processes.

Benefits of Business Continuity

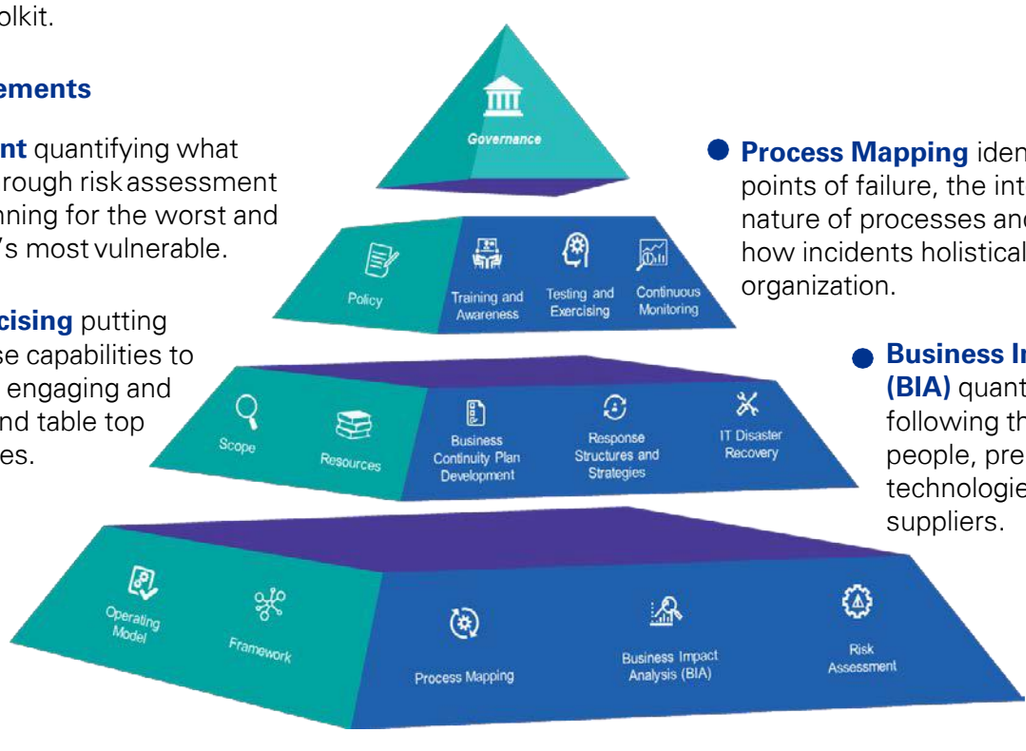
- **Increased resilience** and chance of survival following disruption.
- Improved knowledge of **critical business processes**.
- The **ability to remain operational** when competitors are not.
- Demonstrates **leadership commitment and trust** to employees and clients.
- Enables **visibility of risks** and integrates with the wider risk management of the business.
- Legal, regulatory and supplier **compliance** (if applicable).

How do we achieve this?

Our team will develop a toolkit that can be applied across an organization to achieve it's target state maturity. Elements that align to ISO22301, good practice guidelines and those best suited to the organization's unique situation will be chosen. The pyramid below highlights fundamental elements of an example Business Continuity Management Toolkit.

BCM Toolkit Elements

- **Risk Assessment** quantifying what matters most through risk assessment techniques. Planning for the worst and protecting what's most vulnerable.
- **Testing & Exercising** putting incident response capabilities to the test through engaging and interactive live and table top scenario exercises.

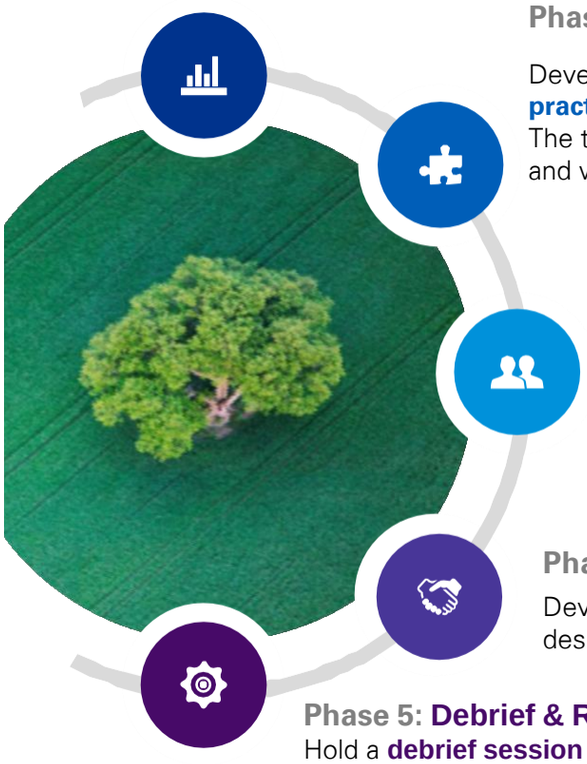


- **Process Mapping** identifying single points of failure, the interconnected nature of processes and understanding how incidents holistically impact the organization.
- **Business Impact Analysis (BIA)** quantifying the impact following the loss of key people, premises, technologies, equipment and suppliers.
- **Business Continuity Plans (BCPs)** providing sites and business functions with a business continuity plan for when incidents occur.

KPMG's Approach

Phase 1: **Discovery Exercise**

Current State Assessment - Review the current state of BCM with **Stakeholder Sessions**, **Document Review** producing a **High Level Executive Summary** containing key gaps and findings.
BCM Target State Workshop – Covering **Industry Insights** and establishing the **target state maturity**.



Phase 2: **Toolkit Design & Build**

Develop a **BCM toolkit** that is **aligned to ISO22301**, **industry good practice** and the size, scale, culture and complexity of your organization. The toolkit will be designed with existing governance structures in mind and will look to fit in with existing practices.

Phase 3: Optional **Pilot Implementation**

KPMG to hold a **pilot implementation** of the strategy, **upskill relevant stakeholders** and prepare them for further employment of the project plan.

Phase 4: **Implementation Project Plan**

Develop a **prioritized implementation project plan** to achieve the desired target state for Business Continuity.

Phase 5: **Debrief & Review**

Hold a **debrief session** with relevant stakeholders to summarise findings, and provide a **detailed review** including recommendations to further enhanced maturity.

"Our security and risk team have been working with KPMG for over three years now. We rely on them to deliver to the highest standards and within demanding timelines.

They consistently demonstrate a good understanding of our business and integrate very well with our teams."

Discovery	Design & Build	Implementation	Debrief & Review
- Current state of BCM - Document review - Industry insights	- Develop BCM toolkit aligned with ISO22301, fitting in with existing practises	- Optional pilot implementation - Full implementation plan to achieve results	- Summarise findings - Detailed review - Recommendations

USCR - Unified Security & Crisis Resilience Model

What is USCR?

USCR is a holistic red team and crisis management service model, which involves exposing vulnerabilities, testing incident response plans and providing roadmaps for remediation of an organization's cyber defences, critical operations, and crisis management capabilities. USCR works by identifying an organization's system vulnerabilities and security flaws. The outputs of this assessment allow for the purposeful creation of a ''live'' cyber-focused crisis event.

How do we achieve this?

Threat Intelligence

Our multi-disciplinary team utilizes all sources of information to produce a **comprehensive intelligence report** on your organization.

Red Teaming

Our team uses intelligence gathered to **identify attack vectors** and entry points into your systems.

We devise strategies **to implement sophisticated attacks** delivered through simulated war-gaming activities within a controlled testing framework.

Crisis Management

We use a series of independent cyber security simulations to test an organization's cyber incident response, business and board crisis management procedures when faced with a cyber focused disruption scenario.

We provide an **immersive training opportunity** for your cyber defence and crisis management teams in a realistic environment.

We provide recommendations on how vulnerabilities can be remediated to **better protect your organization**.

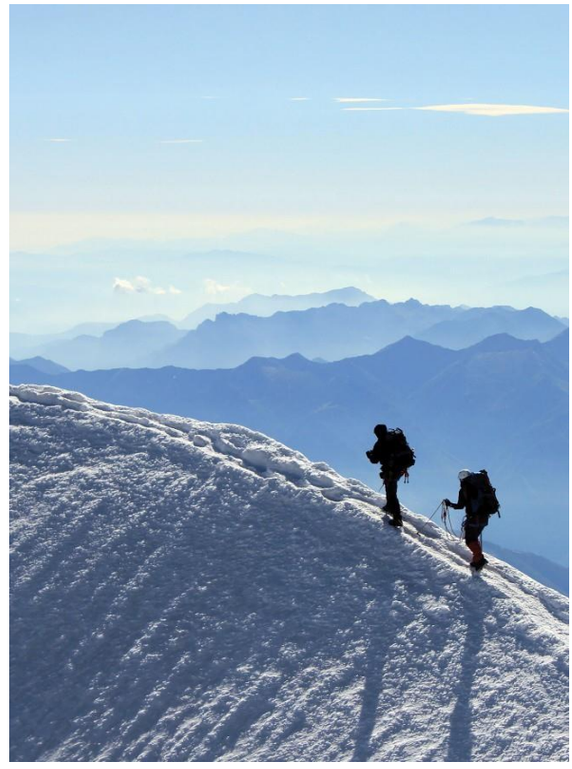
Why do you need it?

It is no longer a question of 'if' a cyber attack will happen to your business, but 'when' an attack will happen. **Your organization will be targeted and you need to be prepared** to effectively manage a crisis situation.

A **realistic attack scenario tests the competencies** of your organization's Incident Response (IR) teams and/or Security Operations Centre (SOC). Escalation to a 'crisis situation' allows us to **assess your Crisis Management teams.**

Benefits of USCR

- Leverages the breadth of **threat intelligence** gathered by KPMG professionals
- Identifies **attack vectors** that criminals may employ to extract data from your organization
- Provides **visibility** into your organization's digital footprint and exposure to data harvesting
- Provides knowledge & warning signs to **harden your systems** to better resist an attack
- Measures the **resilience** of your organization's cyber defences and qualifies the effectiveness of your organization's security awareness program
- Matures your **strategic** crisis management capabilities and readiness.
- Provides a **practical training opportunity** for your crisis management and cyber defence teams



KPMG Approach

Phase 0: Gather Intelligence and Jointly Establish Red Flags

- Our team will conduct a threat intelligence investigation to ensure we fully understand your business model and technical systems.
- This will allow us to create tailor-made scenarios to provide the most realistic picture of your organization's security posture.
- We will jointly establish Red Flags. These represent targets real hackers might be interested in.
- We will select targets on your external surface and determine appropriate attack methods.

Phase 1: System Compromise

a) Weaponization

– We will develop attack methods by finding existing or developing new exploitation methods for found weaknesses. .

b) Delivery

- Our team will implement the attack vectors in the most realistic way possible.
- We will test your resilience against various manipulative cybercrime delivery methods.

c) Exploitation

– Our team will gain access to your organization's infrastructure to complete a successful attack path.

d) Installation, Control & Persistence

– We will install malicious software to persistently and remotely control specific machines in your organization's infrastructure, while evading suspicion.

Throughout Phase 1 - Defence Evasion

– We will test your organization's detection capability, specifically what technical and behavioural command and control patterns were identified.

Phase 2: Network Propagation

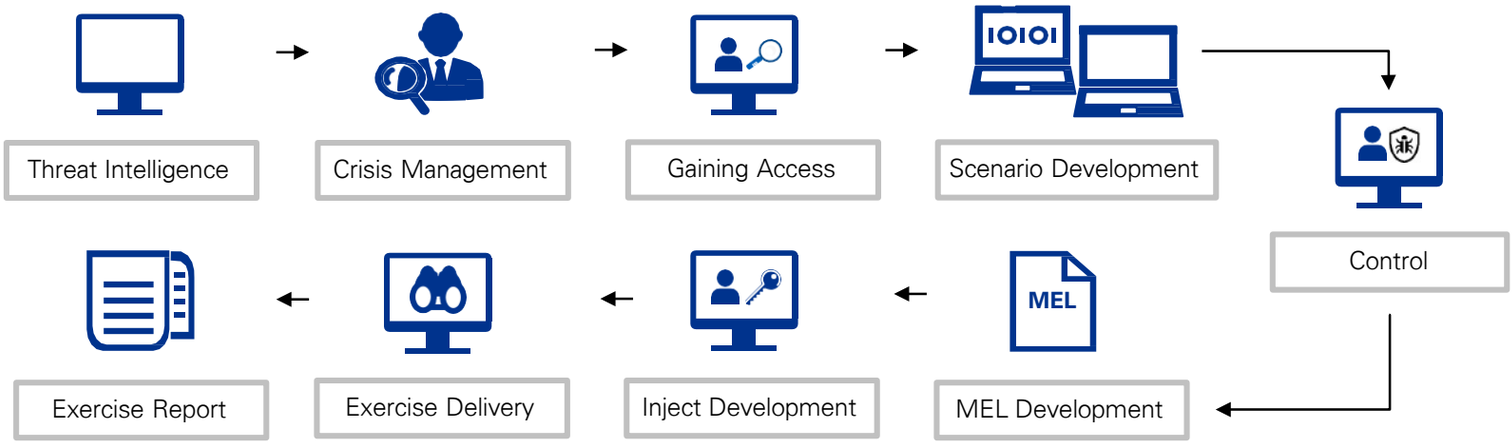
- Our team will attempt to move laterally across your network via accessing credentials and privilege escalation.
- We will be in a position within your network where we can access information or systems identified during Phase 0.
- We will compile reports regarding what vulnerabilities our team identified and successful attack paths we employed.

Phase 3: Action on Objectives

- Our team will work on the collection and exfiltration of information we have accessed to reach objectives set out in the kick off meetings.
- We will not always focus on accessing data. Our exercises can focus on accessing pre-approved target systems in an Operational Technology environment.

Deliverables

- We will produce an overview of the exercise, observations and recommendations for improvement, conclusions, and next steps, accompanied by raw data collected throughout the exercise and a full list of exercise participants.
- We will take regular logs and screenshots to evidence our approach.
- We will provide you with advice on how to improve your organization's cyber resilience.



Contact us

Akhilesh Tuteja
Partner and Head
Risk Consulting - KPMG in India
Co-Leader Global Cyber Security
T: +91 98710 25500
E: atuteja@kpmg.com

Ritesh Tiwari
Partner and Head
Risk Consulting Markets
KPMG in India
T: +91 85888 62899
E: riteshtiwari@kpmg.com

Atul Gupta
Partner and Head
IT Advisory;
Cyber Security Leader
KPMG in India
T: +91 9810 081050
E: atulgupta@kpmg.com