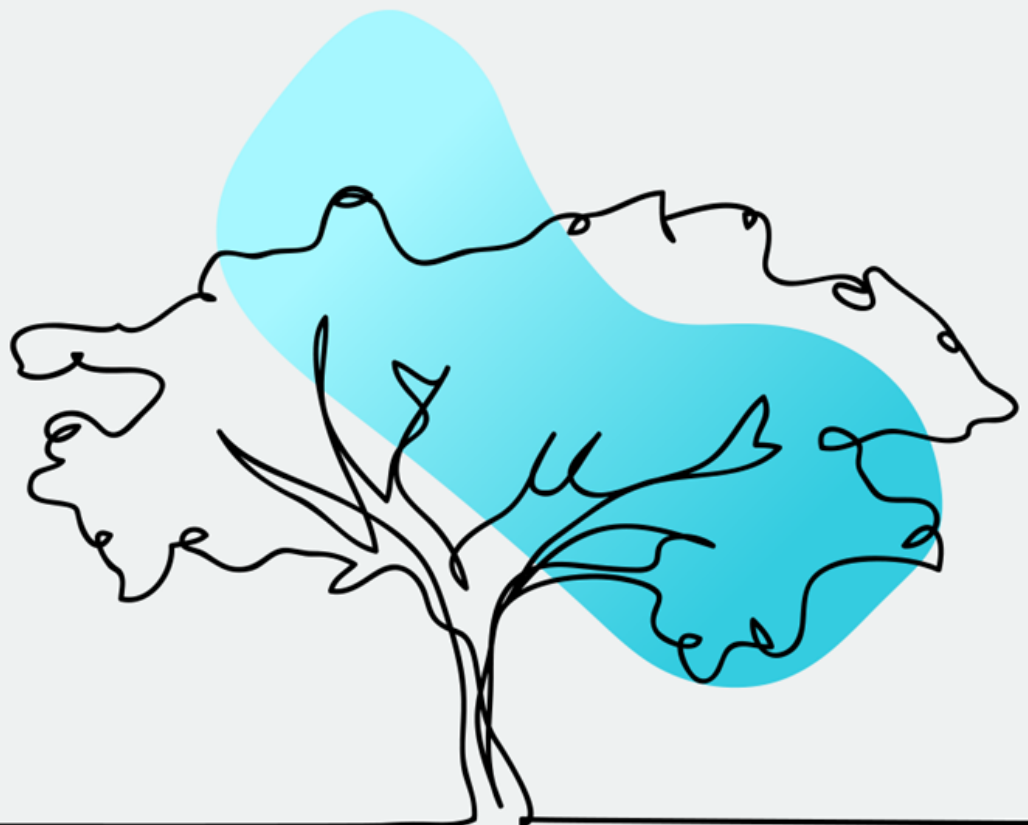




Crisis Management & Business Continuity Guide



Contents

| | |
|----------------------------------|----------|
| Introduction | 3 |
| Crisis Management Program | 4 |
| Business Continuity | 6 |
| Contact Us | 8 |

Introduction

KPMG can support your organization:



Crisis Management Program

KPMG designs and delivers 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 designs and delivers 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.

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 cyber peril**.
-  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: Mobilization

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

Phase 1: Exercise Preparation

- Kick off meeting to agree on 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 3: Exercise Delivery

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

Phase 2: Exercise Design

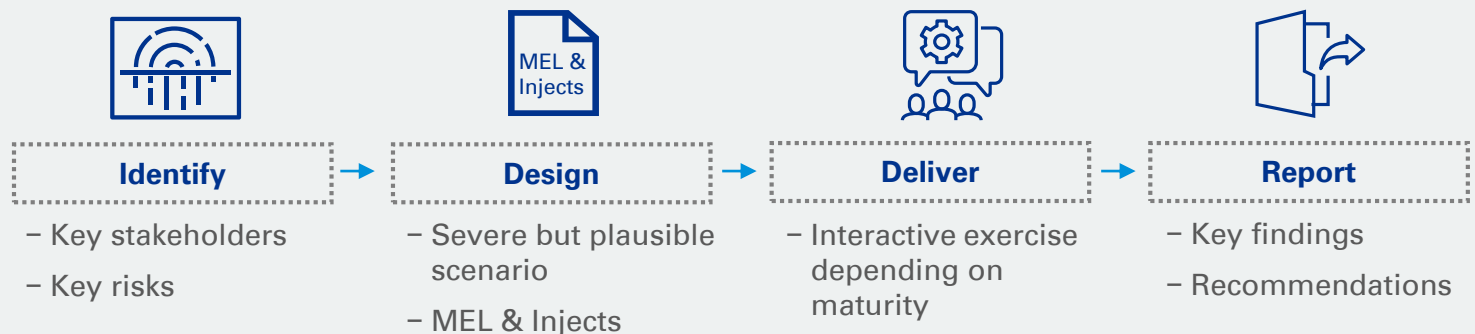
- Hold workshops with SME(s) to develop and agree final scenario.
- Produce a Master Events List (MEL) and injects to support scenario.
- Hold a Dry Run to finalize the MEL and injects created.
- Finalize attendees and logistics.

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?

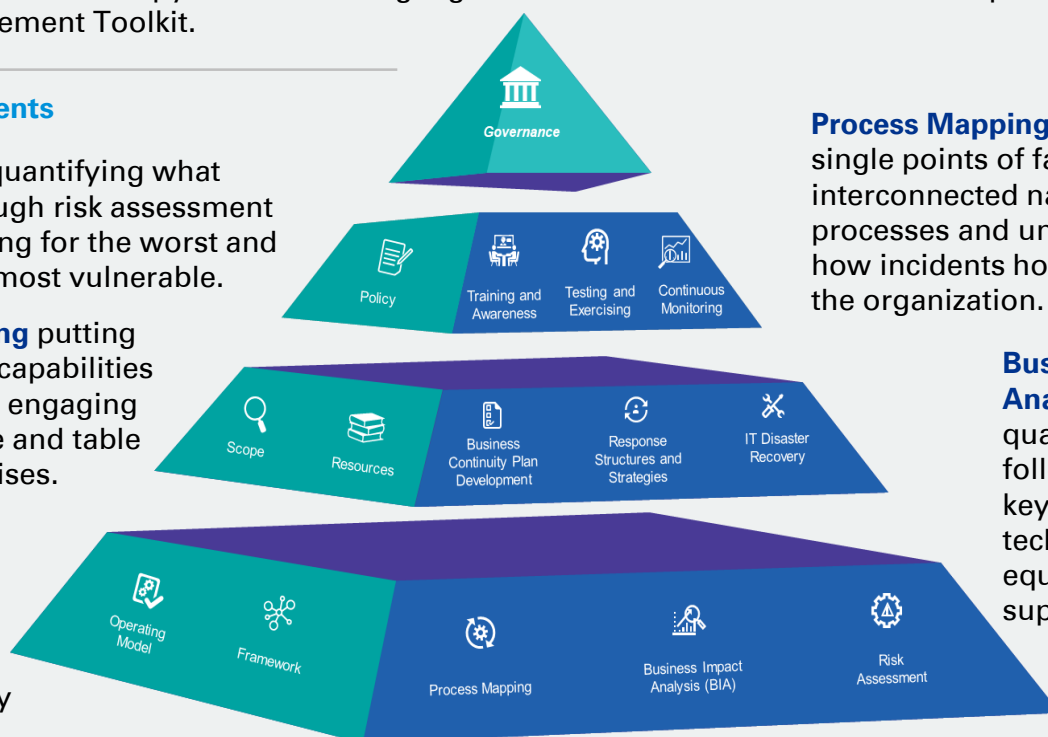
Our team will develop a toolkit that can be applied across an organization to achieve its target state maturity. Elements that align to ISO22301, good practice guidelines and those best suited to the organization's unique situation will be chosen. The pyramid below highlights fundamental elements of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

Business Continuity Plans (BCPs) providing sites and business functions with a business continuity plan for when incidents occur.



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.

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 standards, 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 summarize 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 high standards and within demanding timelines. They consistently demonstrate a good understanding of our business and integrate well with our teams”.



Discovery

- Current state of BCM
- Document review
- Industry insights



Design & Build

- Develop BCM toolkit aligned with ISO22301, fitting in with existing practises



Implementation

- Optional pilot implementation
- Full implementation plan to achieve results



Debrief & Review

- Summarise findings
- Detailed review
- Recommendations

Contact us

Doron Telem

National Leader, Risk Consulting
416-777-3815
dorontelem@kpmg.ca

Kareem Sadek

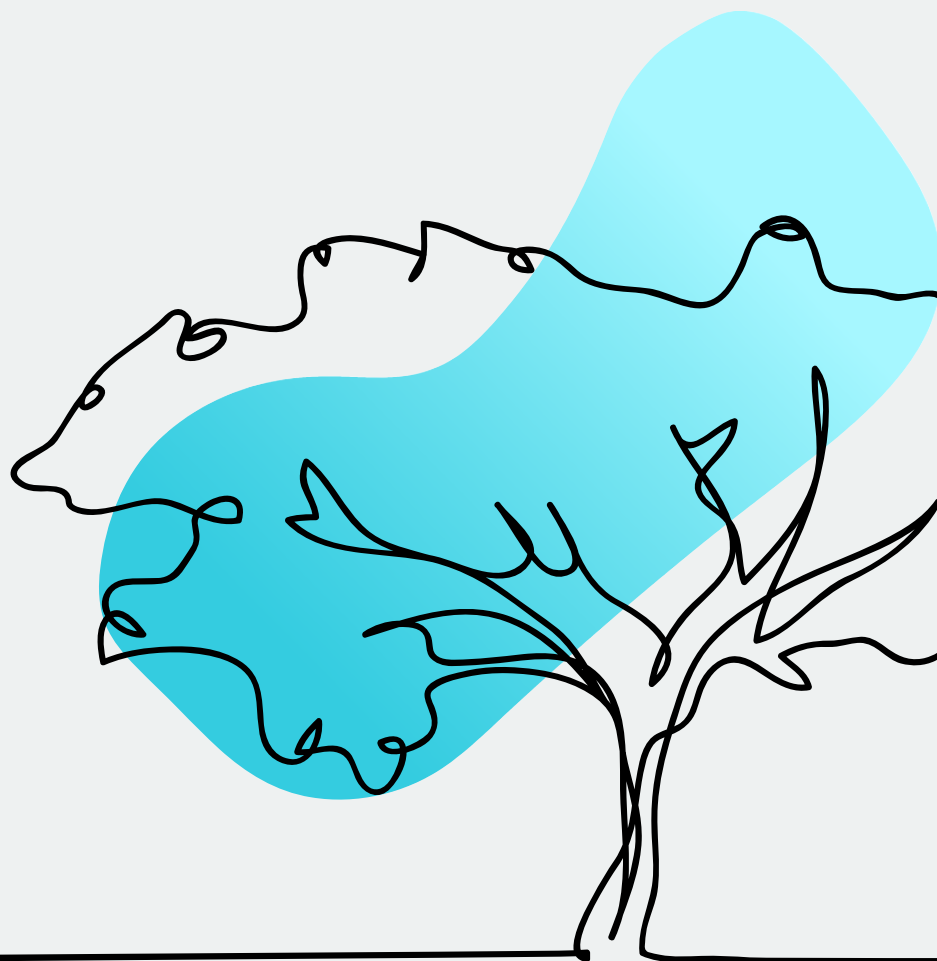
Partner, Risk Consulting
416-777-3446
ksadek@kpmg.ca

Hartaj Nijjar

Partner, Risk Consulting
416-228-7007
hnijjar@kpmg.ca

Dave Knott

Senior Manager, Risk Consulting
416-777- 8654
dknott@kpmg.ca



[kpmg.ca](https://www.kpmg.ca)



© 2020 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the United Kingdom. The KPMG name and logo are registered trademarks or trademarks of KPMG International. 26744

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.