Managing risk through resilience to recovery

COVID-19 issues and solutions

April 2020
The rapid outbreak of the coronavirus presents an alarming health crisis – in addition to a human impact, a significant commercial impact is being felt globally. 

Click below to read insights by our subject matter specialists, to help position your business to be resilient in the face of this and the next global threat.

Table of contents

<table>
<thead>
<tr>
<th>Crisis management &amp; business continuity guide</th>
<th>COVID-19: What the CIO and CISO can do to help</th>
<th>Business continuity support</th>
<th>Orchestrating a resilient digital risk program</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>10</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>Managing third party risks during COVID-19</td>
<td>Challenges &amp; considerations for effective internal controls over financial reporting</td>
<td>Insurance claim services for COVID-19 affected businesses</td>
<td>COVID-19: Digital employee crisis management</td>
</tr>
<tr>
<td>20</td>
<td>22</td>
<td>25</td>
<td>27</td>
</tr>
<tr>
<td>COVID-19: The impact on internal audit</td>
<td>Retail in a COVID-19 world</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>33</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 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 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 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 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.

---

**Identify**

- Key stakeholders
- Key risks

**Design**

- Severe but plausible scenario
- MEL & Injects

**Deliver**

- Interactive exercise depending on maturity

**Report**

- Key findings
- Recommendations
Crisis management program

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?

A Crisis Management Program allows an organization to:

- 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 a crisis management program

- 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”.

Contact us

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

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

Myriam Duguay  
Partner, Risk Consulting  
514-840-2161  
myriamduguay@kpmg.ca

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

Design & Build  
- Develop BCM toolkit aligned with ISO22301, fitting in with existing practices

Implementation  
- Optional pilot implementation  
- Full implementation plan to achieve results

Debrief & Review  
- Summarise findings  
- Detailed review  
- Recommendations

© 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.
COVID-19: What the CIO and CISO can do to help

Concern over the scale and impact of the COVID-19 pandemic is growing, leading organizations to consider their response and the actions they need to take to maintain their business. The CIO and CISO have vital roles in making sure an organization can function as pandemic containment measures are implemented. KPMG in Canada has put together a list of key considerations and questions to help navigate these challenging times. We also address five security domains that should be considered in the COVID-19 era.

**Can your business function effectively through remote working?**

You need to ensure your business can work remotely and flexibly, and that employees are confident in being able to do so. This may require you to revisit decisions on access rights, entitlements and risk posture. Questions to consider:

- Have you scaled your VPN concentrators, portals and gateways to handle a large number of colleagues who will need to work remotely?
- Have you considered who will need to have access and the additional scale that this will bring in? Have you tested the infrastructure to find out whether it can handle the expected loading?
- Are there single points of failure in the infrastructure, and can you provide additional resilience?
- Do you need to relax access controls or provide additional remote login accounts or credentials?
- Is there sufficient help desk capacity to handle any queries from users who are unable to login, or unfamiliar with remote working?
- Where employees require access to laptops for remote working, is there a pool of laptops available or can more be procured and installed to meet demand, and how should allocation be prioritized?
- In cases where the pool of equipment is limited, have you considered essential services and splitting access to them via alternative access solutions (e.g., O365 and One Drive vs. in-house applications)?
- Have you considered the ability to whitelist only specific applications during this period and block all non-essential services?
– Do you have limitations on video and audio teleconferencing bridges, and can you do anything to scale that infrastructure?
– Do you need to consider alternate cloud-based conferencing and teleworking solutions?
– Do all members of staff have the necessary access numbers/links to allow them to access the bridges; is training material readily available; should you establish a helpline?
– Can you remote your help desk operations if the help desk staff have to work from home?
– Have you prepared simple guides to be distributed to staff on key help desk related queries:
  – How do I login?
  – How do I change my password?
  – How do I access key services?
  – How can I get help from the help desk?
  – Who are my key contacts if I have a crisis?

Working from home securely amidst COVID-19
– Remote workers have access to data, information, and network resources. This will attract imminent attention from bad actors.
– Expect an increase in phishing attempts, especially targeted attempts towards VIP credentials. Be wary of requests that break corporate policy.
– Be wary of anything “urging you” to access information via a third-party or attachment files, especially if it is related to COVID-19.

Cybersecurity considerations

1. **Use only trusted Wi-Fi networks, and be mindful of the risk.**

2. **Use precautions when in public; there is increased risk of device and data theft (all connections should be encrypted).**

3. **Only use sanctioned company devices and services for handling company data (use a VPN):**
  – Use approved work-from-home technologies.
  – Use a company private network resource (VPN).
  – Do not use third-party services because you can’t access your standard systems.
  – Use approved systems and services to communicate and transfer information. For example, do not use Dropbox to transfer a document to a client because you can’t access your standard security system or service.

4. **If you require company devices to work from home, ensure the following:**
  – A formal approval from technology staff to borrow devices.
  – An assurance that required security software is properly installed.
  – Use of VPN and encryption where possible to protect data at rest and in transit, for files, systems, and general communications.

5. **Personal devices are generally against most organizations usage policies, but if special approval has been provided to perform work tasks, ensure the following:**
  – Systems are completely updated.
  – Systems and software have current and up-to-date antivirus software.
  – Do not store any unnecessary data (even Office documents).
  – Delete company data from the devices as soon as it is unnecessary.
Watch for phishing attacks – treat Coronavirus – themed emails with great caution:

- Be wary of communications provoking a sense of urgency, particularly those with attachments or links that have “added information”.
- Be wary of the abuse of legitimate brands being used to deliver information related to COVID-19.
- Be wary of communications purporting to come from the Centers for Disease Control and Prevention (CDC) or World Health Organization (WHO).

Are you able to scale digital channels to deal with demand?

Restrictions on travel and the spread of the virus may lead to new patterns of demand, and higher traffic on digital channels.

- More customers and clients may expect to transact with you through digital channels, can you scale those systems and services to deal with changing demand?
- How would you monitor loading and performance, and who can make the decisions to scale capacity, or create dynamic choices on prioritization if capacity is an issue?
- Are you clear which services you may need to shed, or how customer journeys may need to alter if systems are overloaded?

- Are you dependent on key call centers, and if those call centers are closed or inaccessible, can customers and clients interact with you through other channels?
- Is there the option to allow call center staff to work remotely, or to transfer their loads to another call center location?
- Have you considered the interactions between call centers and service/help desks and the impact of any outsourcing arrangements?
- Have you discussed the arrangements with key suppliers of those services, and how will they prioritize your needs against those of other clients?

Are you dependent on key IT personnel?

- Sadly, employees may be infected or may find themselves unable to travel or to have to meet family caring commitments; you should plan for a significant level of absenteeism.
- What would happen if key IT personnel (including contractors) are unable to travel, or are ill with the virus…are you dependent on a small number of key individuals?
- How could you reduce that dependency, for example, ensuring that there are “break glass” procedures in place to allow other administrators access to critical systems?
- What about the Security team? Who are the key individuals, and if the CISO is not available, then who will make the calls on the security posture and the acceptable risks to the firm?
What would happen if disruption to a data centre occurs?

- Data centers may be impacted by the virus too. A positive test may result in an evacuation and deep clean of the building; transport infrastructure disruption may prevent access, and data center staff may be unable to work.
- In the event that one of your data centers is evacuated, do you have disaster recovery plans in place to deal with the disruption, and have you tested those plans?
- How quickly can you failover to an alternate site, and who manages that process?
- Are you dependent on key individuals (including contractor support) for the operation of the data center, and how can you manage that dependency?

Are you able to scale your cloud capabilities?

There may be additional demands on cloud-based services, requiring you to scale the available computing power, which may incur additional costs. Other services may show reduced demand.

- Are you able to monitor the demand for cloud computing services, and manage the allocation of resources effectively?
- Have you made arrangements to meet any additional costs which may be incurred from scaling or provisioning other cloud services?

Are you dependent on specific suppliers?

Your suppliers and partners will also be under pressure, and their operations disrupted too.

- Who are your critical suppliers, and how would you manage if they are unable to operate, including disruption to your key managed service providers?
- Are there steps you could take now to reduce that dependency, including using your team resources?
- Are you discussing the implications with your key suppliers, and do you have the right points of contact with those suppliers?
- Have you identified which IT suppliers may come under financial pressure, and what would be your alternate sourcing strategy if they did fail?

What would happen if there’s a cyber incident?

Organized crime groups are using the fear of COVID-19 to carry out highly targeted spear-phishing campaigns and set up fake websites, leading to an increased risk of a cybersecurity incident.

- Have you made it clear to employees where to get access to definitive information on the COVID-19 pandemic and your firm’s response to COVID-19?
- Have you warned staff of the increased risk of phishing attacks using COVID-19 as a cover story?
- If you’re dependent on alternative systems or solutions, including those procured as cloud services, how would you handle a security incident involving those systems?
- Do you need to change your approach to security operations during the pandemic, including arrangements for monitoring of security events?
What would happen if there’s an IT incident?
While COVID-19 dominates the news, you should still be aware of the possibility of an IT failure given the changing demands on your infrastructure, or an opportunistic cyberattack.

- Would you be able to co-ordinate the incident remotely, and do you have the necessary conferencing facilities and access to incident management sites/processes and guides?
- Do you have a virtual war room setup, in case physical access is limited or restricted?
- Are you dependent on key individuals for the incident response, and if so, what can you do to reduce that dependency?
- How does the emergency/incident response crisis management structure change if key incident managers/ recovery leads are unavailable?
- Are you confident that your backups are current, and that in the worst case you can restore vital corporate data and systems?
- How would you deal with a widespread ransomware incident, when large parts of your workforce are home working?

Are you making the best use of your resources?
You will need to be able to function with limited employee numbers and be clear on the priority tasks your team needs to be able to complete.

- Have you prioritized your team’s activities, are there tasks which you can defer and release staff for contingency planning and priority preparation tasks?
- Do you have the ability to access emergency funds if you need to source equipment, or additional contractor/specialist support rapidly?
- If you are placed under pressure to reduce discretionary spend to preserve cash, are you clear on which spend must be protected and where to make those savings?

Are you setting an example?
Amongst all of these organizational considerations, you are still a member of senior management, and your team will look to you for leadership and support.

- Have you made sure your team is implementing sensible hygiene practices, including offering flexible and remote working to meet changing needs?
- Do you have up to date points of contact details for all of your team? Is your team aware of who to contact in an emergency?
- Do you model the behaviors you expect of your team, and what would happen if you were incapacitated? Who would step in for you?
# Functional domains of cyber operations in the COVID-19 era

## 5 security domains to consider

<table>
<thead>
<tr>
<th>Incident Command and Control must be maintained remote work conditions:</th>
<th>Security monitoring must adapt &amp; persevere:</th>
<th>Response capabilities extend to remote working conditions:</th>
<th>Cyber risks introduced due to remote working conditions and persistent threat actors will continue to evolve:</th>
<th>The Cyber Operations under function now extends to an expanded threat surface:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Ensure redundant communications plan (e.g. employees should be made aware of how to contact security) ✓ Ensure ransomware playbook awareness and revision (e.g. should consider working from home scenarios) ✓ Integrate cyber into crisis management. (e.g. privacy, public affairs)</td>
<td>✓ Ensure all security controls are updated and logging is enabled properly ✓ Ensure remote forensics capability (e.g. remote image collection) ✓ Review use cases for effectiveness as network behavior has changed ✓ Ensure actioning of any lost network visibility due to working from home (e.g. use IDS/IPS)</td>
<td>✓ Ensure vendor contact information and SLAs are reviewed and understood by security personnel ✓ Review emergency change management processes in order to expedite approvals ✓ Ensure user termination processes are functioning end to end (e.g. all access drops upon user termination) ✓ Ensure all administrative actions are logged</td>
<td>✓ Conduct blue team review of email and VPN access control postures ✓ Ensure full review of identity and access management and authentication posture ✓ Monitor perimeter for unintended network exposures ✓ Communicate guidelines for employees to secure their home networks ✓ Ensure all security technologies are being updated as required</td>
<td>✓ Security teams must prepare to operate remotely, but potentially within company infrastructure if cut off from network ✓ Ensure security responders have a secure location and redundant infrastructure where they can respond effectively to more serious cyber events. ✓ Strictly forbid use of unmanaged personal devices for work duties (e.g. home PC) ✓ Review Cyber-Insurance coverage given remote work posture and changing attack surfaces</td>
</tr>
</tbody>
</table>

### ESSENTIAL

- Better Integrate with industry through ISACs

### ENHANCED

- Focused defensive planning of most likely and most dangerous threats given the COVID-19 event
- Better Integrate with industry through ISACs

<table>
<thead>
<tr>
<th>Command</th>
<th>Sense</th>
<th>Act</th>
<th>Shield</th>
<th>Sustain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capabilities to Enable Decision Making and oversee security operations.</td>
<td>Ability to detect cyber events of interest. E.g. Security Controls and SIEM</td>
<td>Ability to contain and remediate an incident once it is discovered</td>
<td>Reactive and proactive hardening of the organization. E.g. vulnerability management</td>
<td>Ability to sustain your cyber posture over the short and long run</td>
</tr>
</tbody>
</table>

---

**Contact us**

<table>
<thead>
<tr>
<th>Hartaj Nijjar</th>
<th>Robert Moerman</th>
<th>Guillaume Clément</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner &amp; National Leader, Cyber Security KPMG in Canada 416-228-7007 <a href="mailto:hnijjar@kpmg.ca">hnijjar@kpmg.ca</a></td>
<td>Partner, Cyber Security KPMG in Canada 416-777-8308 <a href="mailto:rmoerman@kpmg.ca">rmoerman@kpmg.ca</a></td>
<td>Partner, KPMG-Egyde KPMG in Canada 418-265-8734 <a href="mailto:guillaumeclement@kpmg.ca">guillaumeclement@kpmg.ca</a></td>
</tr>
</tbody>
</table>
Your priorities right now are keeping your people safe, delivering services and products, and keeping your businesses afloat.

We understand what you are facing

Many businesses have contingency plans that were developed with an eye on more common disruptions such as power outages, unavailability of facilities, and the downtime of production equipment. However, prolonged disruptions due to unforeseen “once-in-a-lifetime” events with macro-disruption may challenge the adequacy of your plans and the preparedness of your people to deal with them.

Your teams are busy dealing with situations they have never encountered before and many feel overwhelmed. They do not have time to consider what areas are not being addressed because the known issues are so time-consuming.

You are in unchartered territory since there is no playbook, but these challenging times can be navigated successfully.

The help you need, the way you need it

KPMG has the multidisciplinary capability to help your teams not only with enhancing your organizational resilience, but also with the effectiveness of your current response and recovery efforts, providing the experience and capacity you need in these challenging times to reduce the downside impact to your organizations.

We can provide immediate and/or temporary capacity as a managed service or staff augmentation:

- With managed capacity, you determine the amount of support you need based on a pre-negotiated hourly or daily rate. Hold a debrief session to reflect on the participants performance.
- With staff augmentation, you acquire the services of a selected professional(s) with the technical and/or functional expertise you need, typically to support an existing team.
Where we can help

Quick business continuity diagnostic
– Review your response to date, ability to sustain the response for an extended period and identify new or better solutions to continue to manage business disruption
– Identify key risks, potential red flags, and improvement areas.

Business Continuity PMO
– Help you through our Project Management Office (PMO) services to expedite your continuity, response, and recovery initiatives by helping you coordinate, direct, and control your efforts.

Continuity, Incident and Crisis Management
– Leverage our experienced team to augment your business functions in executing your Business Continuity, Incident Response, and Crisis Management plans and ongoing activities

Emergency Cloud Deployment
– Help enable secure access to internal systems and environments not previously available for widespread company-wide remote access.

Recovery Plan Development
– Help you define recovery plans, return to work transition, and operating model changes to resume a “new normal” for business operations

Contact us

Stephanie Terrill
National Leader
Management Consulting
416-777-8994
sterrill@kpmg.ca

Narmin Vasanji
Partner
Management Consulting
403-691-8125
nvasanji@kpmg.ca

Hartaj Nijjar
Partner
Cyber Risk
416 228-7007
nvasanji@kpmg.ca
We understand what you are facing
During the current health crisis, organizations of all sizes are moving into crisis mode: evaluating and prioritizing business critical imperatives, and forcing risk functions to re-evaluate their role to ensure business continuity. A risk-based approach to prioritizing security and privacy is a well understood concept; with the global pandemic, however, these approaches are being put to the test.

CISOs, CROs, CIOs, CSOs continue to focus on protecting the integrity of the business. As digital risk leaders, you are mapping out your critical processes and assets and ensuring systems are in place to protect them – all without compromising critical business functions.

Re-evaluating your risk approach
Many organizations are re-evaluating their risk-based approach to managing digital risk in order to carefully and rapidly respond to the complexity of COVID-19. This can include: immediate recovery from disruptions to core and supporting business operations; rejuvenating risk functions by implementing strategies to rollout “lean” risk practices; and addressing alternative working arrangements.

As more remote workers gain access to data, information, and network resources, expect an imminent rise of attention from bad actors. As your organization’s security posture evolves, so too will your approach to managing digital risk. It is critically important to:

- Re-evaluate your critical assets – with changing work environments, end points and employee access, do we have an accurate picture of our critical assets and their security protocols?
- Re-evaluate risk and reporting benchmarking – are we reporting the right risk and benchmarking metrics given the shifting security and risk landscape of the organization?
- Re-evaluate risk-as-a-service – are we strategically supporting our critical functions and priority initiatives?
- Revitalize resilient risk platforms – are we leveraging technology sufficiently to manage risk identification, monitoring and reporting practices seamlessly across the organization?

The COVID-19 crisis is disrupting and changing the technology risk and security landscape. The role of digital risk leaders – including CIO, CRO, CSO and CISO – in fortifying risk & security while acting as a business enabler is critical.
How we can help

Our KPMG team is a cross functional group that applies risk-based concepts to provide business-focused, technology-enabled skillsets and plug and play solutions to help rapidly orchestrate a resilient digital risk program. Services include:

Out-of-band incident response platform
- Integrated incident response program across BCP/DR, Cyber, Fraud, Physical and other sources
- Deployed with out-of-band network option for minimum business disruption during crisis, breach & outage protocols in effect

Plug & play solutions with orchestrated workflows and incident response playbooks
- Integrated risk management taxonomies for business risk context and insights.

Other digital risk services
- Digital “crown jewel” readiness exercise
- Integrated risk management re-boot (digital risk quantification and remediation)
- Risk-as-service solutions.

Contact us

Sree Kunnath
Partner
Technology Risk
437-237-7934
skunnath@kpmg.ca

Hartaj Nijjar
Partner
Cyber Risk
416 228-7007
nvasanj@kpmg.ca
The COVID-19 pandemic continues to grow with significant impact on the global economy triggering business continuity and crisis management responses across organizations of all sectors and sizes. Organizations relying on third parties to provide critical services should take immediate actions to determine the possible risks these parties may present to their businesses in order to mitigate potential impacts from COVID-19.

### Key considerations for effectively managing your third party risks during COVID-19

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Key Considerations</th>
<th>Potential Response Strategies</th>
</tr>
</thead>
</table>
| Business continuity and resiliency risk | – Are the third party’s business continuity measures working for my organization in the current situation?  
– Is the third party effectively executing business continuity plans and providing urgent deliverables?  
– Is the third party at risk of becoming insolvent?                                                                 | – Are the third party’s business continuity measures working for my organization in the current situation?  
– Is the third party effectively executing business continuity plans and providing urgent deliverables?  
– Is the third party at risk of becoming insolvent?                                                                 |
| IT and cyber risk               | – Does the third party have the technology capabilities to continue providing services in situations like mandatory work from home?  
– Are information and cybersecurity risks being adequately addressed by the third party?                                                                 | – Review third party cyber response strategy to COVID-19  
– In consideration of above response strategy, review potential information security and data privacy impacts |
<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Key Considerations</th>
<th>Potential Response Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key person risk</td>
<td>– What steps have been taken to manage the key person risk at the third party?</td>
<td>– Identify backup personnel for third party relationship</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– as well as critical talent pool impacting third party deliverables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Ensure pandemic plan strategy addresses internal third parties (e.g. contractors)</td>
</tr>
<tr>
<td>Fourth party risk</td>
<td>– How much does my organization know about third party’s reliance on its suppliers and vendors?</td>
<td>– Review the vendor inventory and contracts to identify and confirm fourth parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Discuss potential impact of fourth party business disruptions with your third party service providers</td>
</tr>
<tr>
<td>Inadequate Service provider monitoring</td>
<td>– How can my organization effectively monitor third parties, including their financial stability and performance?</td>
<td>– Establish critical short-term milestones and risk indicators for the third parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Schedule relationship meetings or calls with key third parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Stay aware of potential implications to third parties</td>
</tr>
</tbody>
</table>

KPMG can assist with a Rapid Third Party Risk Assessment to identify the highest risk areas and third parties and suggest critical mitigation actions.

Contact us

**Doron Telem**  
National Leader, Risk Consulting, Chair of KPMG Lighthouse in Canada  
416-777-3815  
dorontelem@kpmg.ca

**Edouard Bertin-Mourot**  
Partner, Risk Consulting  
416-777-3511  
edouardbertinmourot@kpmg.ca

**Hitesh Patel**  
Partner, Forensic and National Co-Lead Financial Crime  
416-777-8191  
hiteshpatel2@kpmg.ca

**Stéphan Drolet**  
Partner and National Forensic Leader  
514-840-2202  
sdrolet@kpmg.ca

**Éric Lachapelle**  
Partner, Forensic and National Co-Lead Financial Crime  
514-840-8365  
ericlachapelle@kpmg.ca

**Kareem Sadek**  
Partner, Risk Consulting  
416-777-3446  
ksadek@kpmg.ca
Background
On March 11, 2020, the World Health Organization declared the Coronavirus COVID-19 outbreak a global pandemic, in recognition of its rapid spread across the globe. In response, many governments have reacted by taking stringent steps in an attempt to contain the virus, including requiring self-isolation/quarantine by those potentially affected, closing borders, “locking down” regions or even countries, and forcing the closure of businesses deemed to be non-essential.

Consequently, these measures have had a significant impact on the way in which many organizations are conducting business, and companies need to consider the potential implications on regulatory compliance, reporting and disclosure, and internal control over financial reporting (ICFR).

Challenges and considerations to effective ICFR

Barriers to obtaining information
Companies with operations in regions experiencing significant effects from the outbreak could face challenges or delays with obtaining relevant financial data for consolidated financial reporting. It is critical for organizations to understand and anticipate where this has the potential to occur, and proactively put measures or additional oversights in place.

Roles and responsibilities
Control owners may not be able to perform their controls due to illness, working remotely or a reduced workforce. Companies will need to examine the existing control structure, and determine whether a re-alignment of roles and responsibilities, or cross-training is necessary.

Material changes in ICFR
With many organizations transitioning to a virtual work environment, companies will need to look at their existing controls and processes and determine whether adjustments and changes will be required to accommodate remote working. For example, new controls may be implemented and/or modified as organizations implement emergency procedures, modify information technology (IT) to enable remote workforces, or account for unanticipated significant events. Companies need to carefully assess whether any such change is considered to be a material change in ICFR, and if so, disclosure would be required, including documentation of all the changes.

Inventory counts and physical asset inspection
If such controls cannot be performed due to working remotely, reduced workforce, or operational shutdowns, companies will need to consider alternatives or other compensating controls that can be relied upon or implemented. For instance, controls
over receipts and requisitions may need to be relied upon more heavily, and tested with greater rigour, and inventory counts may need to be performed after the balance sheet date, in which case rollback procedures will be necessary. Early discussions with the company’s internal and external auditors will be critical in managing the difficulties with inventory counts and physical asset inspection, as external audit standards require physical attendance at inventory counts for material inventory.

**Fraud risk assessment**
Companies will need to assess whether fraud risks have changed as a result of the virtual environment. For instance, reduced visibility and oversight may create a greater opportunity for financial reporting fraud or misappropriation of assets, or the ensuing economic conditions and impact on operational performance may create more incentive for financial reporting fraud.

**Reporting and disclosure matters new to the company**
Economic uncertainties and market volatility have the potential to affect accounting conclusions, and may result in new and emerging accounting and disclosure matters for which controls will need to be implemented. Examples include controls over liquidity analysis and going concern assessment, asset and inventory valuation assessment, commitments for severance costs, unanticipated significant unusual transactions, such as insurance recoveries related to business interruption, or subsequent events accounting and disclosure, in light of the rapidly evolving environment.

**Entity level controls**
Difficulties with directing and supervising work of team members due to a virtual work environment could change the control environment and require changes to the way in which entity level controls are implemented. Examples include direct oversight, means and frequency of communication, monitoring, considerations with respect to compliance and enforcement of the company’s code of conduct, risk assessment process, etc.

**Regulators and filing requirements**
Regulators are extending filing deadlines in response to the business challenges faced by many organizations in light of the current environment. Companies should consider whether they should take advantage of extended filing deadlines, and will also need to continuously monitor information released by regulators on updates to filing requirements and additional relief.

**Cybersecurity**
Companies may face potential increased vulnerability to cyber-attacks due to remote work environments, such as greater susceptibility to phishing attacks and malware. Consequently, organizations will need to think about increasing awareness and education related to cybersecurity, and may need to enhance their security monitoring capabilities to detect threats and potential infections, as well as perform vulnerability assessments and other testing to ensure proper cybersecurity measures are in place.

**Management review controls**
Where there is heavy reliance on review controls that involve trend and predictive analyses, companies should consider whether the predictability of outcomes remains reliable, given the rapidly changing environment. Review controls may require more comprehensive analysis, or probability weighting as opposed to point estimates, which will also necessitate additional documentation to appropriately evidence the performance of the review.

Additionally, there may be circumstances where review controls will need to be relied on more heavily for testing purposes, if easier to test remotely than manual preventative controls. Review controls typically have additional supporting documentation requirements, which companies need to consider in evaluating ICFR.
Evidence and ICFR testing
An important aspect of ICFR is the maintenance of sufficient evidence regarding the performance of a control. There may be changes to the way in which controls are performed in a virtual environment, with more reliance on electronic records and documents. Companies may need to develop a system to appropriately document and evidence the performance of a control, in particular where hard copy documents have traditionally been retained as evidence of review. Organizations need to ensure the relevant technology is available to support the changes, and that there are appropriate controls over electronic sign-offs, server access, and protocols are in place for maintaining digital records.

Companies should also consider whether changes in the planned testing approach are needed due to travel restrictions and working remotely, and should develop an approach for testing that is dynamic and responsive to the current environment.

Recommendations and best practices
The following are some key recommendations for companies to consider in assessing and responding to necessary changes to ICFR in light of the current environment:

- Implement an iterative risk assessment process, including fraud risk assessment. Companies will need to revisit their financial reporting risk assessment on an ongoing basis by looking at the financial statements and giving consideration to where new and enhanced accounting and disclosures and ensuing controls, may be required as a result of the ever-evolving circumstances.

- Identify an individual or group to evaluate existing processes and controls and assess what changes are necessary. Do this now!

- Engage those charged with governance.

- Consider whether revisions to reporting requirements may be necessary to accommodate new processes, competing demands on team members, and barriers to obtaining financial data.

- Consider taking advantage of extended reporting deadlines granted by regulators, and continuously monitor information released by regulators with regard to revisions to reporting deadlines and requirements.

How KPMG can help
We have highlighted five areas where KPMG can provide support.

1. **Sounding board:** Provide advice on reviewing and assessing the current state of ICFR, and best practices as you transition and adapt to the new circumstances.

2. **Risk assessment updates, including fraud risk assessment:** Review and assess processes and controls and advise on changes to your risk assessment process.

3. **Internal audit “readiness assessment”:** Perform an assessment of newly implemented processes and controls with the aim of identifying gaps and areas for improvement before new controls are fully implemented.

4. **Designing and documenting new controls and processes:** Update documentation, including process narratives, control descriptions, and risk and control matrices, to reflect changes to the existing control environment.

5. **Internal control evaluation:** Assess the design, implementation and test the operating effectiveness of newly implemented internal controls.

Contact us

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

**Katherine Wetmore**
Partner, Risk Consulting and Audit
647-777-5380
katherinewetmore@kpmg.ca
The COVID-19 outbreak is impacting all of us in a number of ways. Supply chains are being disrupted, businesses are being closed, events cancelled, and combined with “social distancing” and other measures imposed by various levels of government, businesses are experiencing and will continue to experience real financial losses. Employee safety and well-being is the first priority in any business continuity plan. Once these needs are met, business owners and risk managers turn to economic recovery, which includes the challenge of dealing with complex property and business interruption insurance claims and government emergency fund applications.

Check your policy coverage
From an insurance perspective, whether losses arising as a result of the COVID-19 pandemic are covered will vary from one jurisdiction to another and will also depend on specific policy terms, which can vary greatly from policy to policy.

Aspects of the loss may be covered under various insurance policies such as business interruption, commercial general liability, and property. There may also be specific coverage for losses sustained due to infectious diseases and/or in relation to orders by civil authority to shut down operations. As such, policies should be carefully reviewed to assess if coverage is available.
Claims preparation services
KPMG’s services in claims preparation can help an organization respond to even the most complex set of circumstances and relieve the pressure on its business in all affected areas.

A major event such as the COVID-19 pandemic can cause significant business losses. KPMG Forensic can help organizations with efficient and accurate claims preparation and filing to avoid the sorts of payment delays that often arise under complex circumstances. Understanding how an insurer or a government will approach a situation is key to successful claims preparation. Our professionals know how to structure a complete and properly stated claim that can bring forth a rapid response.

KPMG Forensic can advise on all aspects of economic recovery, including

- Assessing the initial loss impact to the business
- The claims process: what to expect, who should be involved, duration, common roadblocks, cash advances, and settlement
- Documentation generally required from insurance carriers and/or government fund administrators in connection with business interruption losses, as well as extra expenses incurred
- Assisting an organization in securing timely progress payments prior to full and final settlement to minimize working capital investment
- Assisting an organization with determination of the indemnity period
- Identifying and quantifying lost sales and customers
- Establishing historical budget trends and analyzing economic factors

KPMG resources
To effectively serve organizations affected by disasters, KPMG has a team of Forensic Advisory professionals that specialize in management and support of first-party property damage and business interruption insurance claims.

This team is prepared to assist companies with insurance claims and/or, government emergency funding applications, helping them quantify the financial impact of the damage they have suffered, and recover their losses.

KPMG Forensic is recognized as a world leader in Forensic and Dispute Advisory Services. We have a multi-disciplinary team with a wide range of experience in assisting clients through the claims processes. We know how to achieve results in an ethical, efficient, and professional manner.

Contact us
For more information or to discuss how we can help you, please contact us:

Kas Rehman  
Partner, Forensic  
613-212-3689  
kasrehman@kpmg.ca

Karen Grogan  
Partner, Forensic  
519-747-8223  
kgrogan@kpmg.ca

David Bushell  
Senior Manager, Forensic  
519-747-8882  
dbushell@kpmg.ca

Peter Mackenzie  
Senior Manager, Forensic  
519-747-8253  
pmackenzie@kpmg.ca

Glenn Smith  
Senior Manager, Forensic  
613-212-3668  
gksmith@kpmg.ca

Michael Kohut  
Manager, Forensic  
613-350-1267  
mkohut@kpmg.ca
The COVID-19 global pandemic has reached a critical phase where events are unfolding with astounding speed, and the picture is changing on a daily basis. This has fundamentally changed business models from office-centric to widely dispersed, decentralized models which has added further stress on the economy and has resulted in organizations scrambling to share information with their teams, customers and vendors. In today’s highly transparent knowledge economy, leaders’ success is being measured internally and externally on their ability to effectively gather, analyze and disseminate information to all business stakeholders. We are working with our global alliance partner ServiceNow® to help organizations who are looking for ways to rapidly deploy tools and adapt in real time.

**Being vigilant about employee matters during a crisis**

As organizations attempt to “flatten the curve” within their workforces by practicing social distancing, yours may be one of many experiencing challenges when attempting to:

- Engage with, and provide critical information, to your employees and other stakeholders
- Support employees who are ill and may be showing symptoms of the virus
- Assist employees who were traveling abroad and are having difficulty returning to Canada
- Track interactions internally and externally when an employee is diagnosed with COVID-19

In an effort to support organizations and help their employees navigate this pandemic, ServiceNow® has launched four COVID-19 Rapid Response Initiative applications and waived their licensing costs to organizations for 120 days. As an existing customer, you can streamline and automate activities across multiple fronts, keeping your employees and stakeholders informed and connected as they anticipate or experience situations that require monitoring emergencies.
ACE COVID-19 Rapid response initiative applications

1. **Emergency Outreach: Keep your employees connected and informed**

This will allow businesses to reach out to their employees through email or the ServiceNow® mobile push notification capabilities to provide critical information.

It can be used to deploy safety measures, request a response to confirm if the employees are safe, confirm staffing locations, and much more. Businesses can also provide daily updates regarding COVID-19, workplace recommendations, and collect updates during these dynamic situations. This application is reasonably simple to implement and integrate into most organizations, particularly those with a ServiceNow® platform in place.

2. **Emergency Self-Report: Monitor your employee’s health status**

This application allows employees to self-identify if they are going into quarantine, and can help organizations track when employees can safely return to work, making staff scheduling easier. Managers, HR and response teams are also enabled to monitor the status of their teams and take appropriate actions through workflows, e.g., reassigning work to their teams as needed. Response teams can get a rollup of the reports, sort the data in multiple ways for analysis, and drill down into the details. Employees who are stuck in another country can also use this app to check in with their employer.

This will provide your HR and management teams with important information in real-time, enabling them to make critical decisions. This application is also reasonably simple to implement and integrate into most organizations, particularly those with a ServiceNow platform in place.

3. **Emergency Exposure Management: Track possible exposure between employees**

In the event that an employee has been diagnosed with COVID-19, this application can assist businesses with identifying other people who may have been exposed to the virus based on the employee’s meetings and locations visited. It is rare that many organizations have the ability to perform contact tracing for employees natively using existing technology. However, this application leverages dynamic data sources, such as Microsoft Office 365 meeting data and employee location, which is available to identify cohorts that may have been in contact with the infected employee. With this knowledge, leaders are able to identify “employee zero” and correlate the broader impact on the organization and the broader community. Tools such as this can help with slowing transmission of COVID-19, ensure timely safeguards are being implemented.

Once implemented, this tool can also be leveraged as part of a broader employee response program for potentially notifying affected employees, customers and stakeholders, thereby helping each group to better respond accordingly and help maintain brand reputation.

This application will require some effort with regards to integration with real-time and manual data content; the KPMG ServiceNow® team is able to outline how this can be implemented in a rapid deployment approach to help organizations get the benefit of this immediately.
4. **Emergency Response Operations: Plan and coordinate emergency responses**

This final application is a more holistic version of the other offerings and was originally derived from a custom application built by the State of Washington Department of Health (DOH) in the Now Platform®. The DOH needed a statewide system that was quick to deploy and could be used to capture needs, information and address previously unstructured, cumbersome and error-prone processes and workflows to provide real-time visibility into resource and staffing allocations. Working with the ServiceNow® platform, over a three week period, the DOH modernized workflows, connected people and improved the way data related to COVID-19 was collected, processed and analyzed. It allowed them to optimize resources in critical locations statewide during emergencies and simplify role assignments and resource activation during incident planning. They continue to evolve the solution as new needs and data is identified.

Organizations that need to implement a comprehensive system that can scale globally to accommodate their business operations can do so with a similar approach. Given the significant interdependencies and integrations, KPMG would work with you to get the platform in place and enable new functionality in very short order. From there we would continue to work with you to ensure that the solution is fully operationalized in your organization. This application would require a medium level of effort over a very short period of time.

**Enabling crises response management**

If you have any questions relating to the ACE COVID-19 Rapid Response Initiative applications, please contact us.

**Contact us**

**Louie Velocci**  
Partner, ServiceNow Advisory Services  
National practice leader  
902-492-6012  
lvelocci@kpmg.ca

**Jason D. Souliere**  
Partner, ServiceNow Advisory Services  
647-777-5480  
jsouliere@kpmg.ca

**Karsten Hiemstra**  
Partner, ServiceNow Advisory Services  
250-244-0857  
khiemstra@kpmg.ca

**Sree Kunnath**  
Partner, Technology Risk  
416-791-2001  
skunnath@kpmg.ca
COVID-19: The impact on internal audit

Responding to disruption and uncertainty

Over the last several weeks, the COVID-19 pandemic has had a disruptive and devastating effect on people across the globe. It has impacted the capital markets, travel and our collective psyche.

How should internal audit respond?

We are currently in unprecedented times, and organizations are facing tough decisions every day to manage through the pandemic. In these times, there are a number of different things to consider, and we have pulled together a few ways internal audit can help provide assurance and insights to Senior Management and the Board.

<table>
<thead>
<tr>
<th>Key actions</th>
<th>Points to consider</th>
</tr>
</thead>
</table>
| Risk assessment        | - During these times, many organizations are facing new risks and challenges. Organizational changes as a result of this pandemic create an opportunity to refine and enhance risk management processes to better protect the organization.  
                         | - Look at risks in the current environment. How are they mitigated and are there any remaining gaps?                                                
                         | - Is the organization venturing into new products and services as a result of COVID-19? What new risks apply?                                      |
| Fraud risk             | - As processes are changed or adapted to accommodate remote working or other operational changes, review key processes for fraud risk, and identify any unmitigated gaps. |
| Annual plan reassessment | - Take time to scrutinize your plans and reprioritize any upcoming audits based on their significance, regulatory requirements and the ability to execute them in a potentially disrupted environment. |
 | | - Review your annual internal audit plan and assess what changes are required. Reschedule or adapt audits to accommodate remote working and barriers to obtaining information. |

© 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.
<table>
<thead>
<tr>
<th>Key actions</th>
<th>Points to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk analytics and benchmarking</strong></td>
<td>As the situation evolves and travel restrictions change, consider how to complete audits without physical access to corporate locations. Careful consideration should be given to performing data analysis utilizing centralized source systems to execute internal audits without the need for a traditional site visit. For example, the use of analytics may involve evaluating locations or processes that exhibit a more mature control environment based on historical performance compared to those which present more risk to the organization.</td>
</tr>
</tbody>
</table>
| **Optimizing labour**              | - Strategize how best to use the team’s time. Challenge your team to work and think differently.  
- Reach out to key business leaders and offer their team’s assistance. For example, your organization may be diverting critical facility operations to another location or creating redundancies in its supply chain for scale. There may be additional risk factors in these operational changes that need to be considered.  
- Internal audit resources may need to be redeployed to support the business’ internal controls over financial reporting programs and testing. |
| **Remote working**                 | - Evaluate your organization’s plans to mobilize a remote workforce, consider key risks and the impact to systems and technologies. Assess IT security and system access risk as roles change due to redeployment.  
- It is important to maintain clear and consistent lines of communication with audit teams and provide reminders to carry out the necessary actions to protect themselves and their families.  
- If an internal audit team can not physically visit a site, think of creative ways to still gain risk coverage. For example, if production plants have video surveillance, would internal audit be able to use those feeds to check whether critical physical controls are still working?  
- Consider the impact of remote working on the organization’s culture risk. Plan virtual team-building and socializing. Set aside time to catch up on each other’s personal lives. Create an open format where people enjoy sharing recent experiences that allows for that sense of belonging to feel like part of the team. |
| **Business continuity planning (BCP)** | - Internal audit should support the business as it implements business continuity, pandemic or crisis management plans.  
- Internal audit should be represented on any crisis management teams. The experience, tools and views of the internal audit department may be invaluable in developing such plans. |
<table>
<thead>
<tr>
<th>Key actions</th>
<th>Points to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber security</td>
<td>– Companies may face potential increased vulnerability to cyber-attacks due to remote work environments, such as greater susceptibility to phishing and malware. Does this impact your risk and audit plans?</td>
</tr>
<tr>
<td></td>
<td>– As more transactions move online, consider the impact to data security risk.</td>
</tr>
<tr>
<td>Supply chain</td>
<td>– Evaluate processes in place to maintain and manage key supplier relationships and identify supply chain risks.</td>
</tr>
<tr>
<td>Major project changes</td>
<td>– Internal audit should support the business as the organization embarks on new major projects or postpones existing projects.</td>
</tr>
<tr>
<td>Third party risk</td>
<td>– Reassess the organization’s third and fourth party risk and consider the impact on the organization’s overall risk assessment.</td>
</tr>
<tr>
<td>Post-crisis review</td>
<td>– Look back on how the organization responded, opportunities for improvement and overall enhancements to crisis management.</td>
</tr>
</tbody>
</table>

**How KPMG can help**

We have highlighted some of the areas where KPMG can provide support:

1. **Sounding board:** Provide advice on reviewing and assessing your internal audit plan, and best practices as you transition and adapt to the new circumstances.

2. **Risk assessment updates, including fraud risk assessment:** Review and assess changes within the organization and advise on changes to your risk assessment process and your annual internal audit plan.

3. **Update documentation:** Including risk registers, risk and control matrices, internal audit plan and internal audit schedule to reflect changes to the organization and the control environment.

4. **Execution of internal audit plan:** Provide resources to support you in executing and completing your internal audit plan.

5. **Changes to approach:** Provide advice and recommendations to your planned audit procedures, including how data and analytics can be used as alternatives to traditional testing.

**Contact us**

**Doron Telem**  
National Leader  
Risk Consulting  
416-777-3815  
dorontelem@kpmg.ca

**Bruce Willis**  
Internal Audit,  
Risk & Compliance  
Service Line Leader  
306-791-1209  
brucewillis@kpmg.ca

**Angela Moch**  
Internal Audit  
Risk & Compliance GTA Leader  
416-777-8093  
amoch@kpmg.ca
As consumer behaviours shift around the globe to help flatten the curve, retailers are scrambling to adapt. They recognize the global response to the COVID-19 pandemic will have a significant impact on their business. They understand the situation is changing daily and that they have little time to respond.

What does all this change, opportunity and risk mean for your organization?

KPMG’s experienced team of Tax, Audit and Advisory professionals have been working with clients around the world to help with a variety of issues arising from this crisis. We have highlighted some of the areas impacting retailers during the current pandemic, and composed a list of important questions and consideration that retail leaders need to be taking into account.

<table>
<thead>
<tr>
<th>Operational</th>
<th>Financial</th>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber security</strong></td>
<td>– As more transactions move online, do you have the appropriate controls in place to maintain data security?</td>
<td>– With an increase to your virtual workforce, is your data secure?</td>
</tr>
<tr>
<td></td>
<td>– With an increase to your virtual workforce, is your data secure?</td>
<td>– Expect an increase in phishing attempts – how are you educating your teams on policies and protocols?</td>
</tr>
<tr>
<td><strong>Business continuity plan</strong></td>
<td>– As you enact parts of your BCP, what processes and controls need to be changed to ensure the business can operate?</td>
<td>– Will some controls need to be relaxed?</td>
</tr>
<tr>
<td></td>
<td>– Will some controls need to be relaxed?</td>
<td>– How are you assessing that risk?</td>
</tr>
<tr>
<td></td>
<td>– How are you assessing that risk?</td>
<td>– Is there an impact to your internal controls over financial reporting (ICFR) framework?</td>
</tr>
<tr>
<td>Operational</td>
<td>Financial</td>
<td>Accounting</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Optimizing store labour</td>
<td>– As some employees may need to be redeployed, how are you working with HR and IT to ensure team members are appropriately upskilled and that system accesses protocols are maintained?</td>
<td></td>
</tr>
<tr>
<td>Supply chain management</td>
<td>– With disruptions in this process, how are you adjusting levels of inventory?</td>
<td>– Have you updated your return policies to address potential returns as a result of hoarding?</td>
</tr>
<tr>
<td></td>
<td>– Have you updated your return policies to address potential returns as a result of hoarding?</td>
<td>– When considering alternative suppliers, what checks are being undertaken?</td>
</tr>
<tr>
<td></td>
<td>– When considering alternative suppliers, what checks are being undertaken?</td>
<td>– How are you managing quality, credit and ethical risks?</td>
</tr>
<tr>
<td>Managing third-party risk</td>
<td>– Have you identified third-parties critical to maintaining business as usual?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Do they have appropriate business continuity plans, IT and cyber infrastructure and key personnel in place? Is there a fourth party risk?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– fourth party risk?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– What are your systems and controls to monitor?</td>
<td></td>
</tr>
<tr>
<td>Tax considerations</td>
<td>– Tax-related announcements from the various levels of government seem to be coming daily.</td>
<td>– In addition to staying on top of the measures governments are taking with regard to tax deadlines and reliefs, tax-related cash management strategies should be part of your overall cash preservation approach.</td>
</tr>
<tr>
<td>Optimizing working capital</td>
<td>– Strategies to optimize working capital include stretching out payment terms, offsetting payables with receivables where possible and accelerating the conversion of receivables into cash.</td>
<td>– Up-front discussions with vendors may increase the chances of receiving accommodations without putting relationships at risk.</td>
</tr>
<tr>
<td>Financing challenges</td>
<td>– Some companies will face challenges as they look to access financing or refinancing during this crisis.</td>
<td>– While policy makers are encouraging banks to keep lending in order to inject liquidity into the economy, banks will also try to avoid lending money to failing enterprises.</td>
</tr>
<tr>
<td>Operational</td>
<td>Financial</td>
<td>Accounting</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| **Contractual considerations** | – In some circumstances, a party may be able to assert a force majeure event in order to excuse its non-performance under a contract without incurring liability.  
– Determining whether force majeure is available requires a detailed legal analysis of the facts, contract and law governing the contract. | |
| **Cash forecasting** | – With operations impacted, cash maintenance and preservation may become a significant focus in the near term.  
– Forecast cash flows under several different scenarios of crisis duration and identify expenditures that can be delayed or cancelled. | |
| **Inventory valuation** | – Increased risk of inventory write-downs on seasonal items, depending on the duration of store shut-downs.  
– Factors that may need to be considered include new and/or alternative liquidation strategies and pack-up/storage costs. | |
| **Impairment of non-financial assets** | – The deterioration in the economic environment and the increased uncertainty in the macroeconomic and business outlook likely represent a triggering event to test for impairment for many retailers.  
– Challenges in estimating cash flows due to the uncertainty around the nature, severity and duration of virus containment measures. | |
| **Going concern** | – Companies are required to disclose material uncertainties related to events or conditions that may cast significant doubt on their ability to continue as a going concern.  
– Disclosure is also required when no material uncertainties exist but reaching that conclusion involves significant judgment (a ‘close call’). | |
| **Liquidity and risk disclosures** | – Companies should consider their disclosure obligations regarding liquidity and business risks related to the impacts of COVID-19 within the context of their regulatory requirements.  
– Disclosures should be specific to individual circumstances, avoiding broad or generic language. | |
| **Rent concessions** | – Relief or concessions from landlords can take many shapes and forms.  
– Concessions from landlords may result in lease modifications, depending on whether concessions were contemplated in the original lease agreement. | |
KPMG can help you with:

- Financial reporting and disclosure considerations
- Risk assessment and internal control review
- Accessing government funding
- Adapting workforce management
- Securing tax relief

Contact us

Farah Bundeali  
Audit Partner  
416-777-3917  
fbundeali@kpmg.ca

Andy Brown  
Audit Partner  
416-777-8280  
ajbrown@kpmg.ca

Samantha Maloney  
Risk Senior Manager  
416-777-3428  
samanthamaloney@kpmg.ca
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.

© 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. 27042

The KPMG name and logo are registered trademarks or trademarks of KPMG International.