

Building an operationally resilient enterprise – COVID-19

April 2020

The rapid outbreak of the coronavirus has presented an alarming health crisis that the world is grappling with. The speed at which COVID-19 is spreading across the world, and the severity with which it has disrupted the global economy, is unprecedented. COVID-19 is affecting every element of business – from the robustness of supply chain to the stability of the financial markets, the availability of the labour force to the threat of rapidly waning customer demand.

In such an unpredictable environment, the key to business survival is building a resilient enterprise considering aspects such as financial, operational, regulatory and commercial resilience.

- Financial resilience: the ability to withstand financial impact on liquidity
- Operational resilience: the ability to withstand operational shocks and continue to deliver the core business
- Regulatory resilience: the ability to continuously comply to regulations applicable
- Commercial resilience: the ability to respond to changing market and consumer pressures.

This point of view sets out challenges that organisations are facing, key lessons learnt and

views on short and long terms actions businesses should be taking from an operational resilience perspective.

We are sharing our experience and have tried to explore practical ways in which organisations can strengthen and plan a phased response to bolster resilience.

There are various factors organisations consider while developing continuity plans for various types of disasters. Such factors include, but are not limited to, externality, enablers impacted, intensity, predictability, duration, spatial extension, community implications. Pandemics such as COVID-19, however, aren't usual business disruptions. Due to uncertainty regarding the duration, intensity and severity of COVID-19, the existing continuity plans are insufficient for ensuring enterprise resilience during and after the crisis.

Major impacts of COVID-19

- Global GDP could shrink by 0.9 per cent in 2020 instead of growing a projected 2.5 percent¹
- >2 million confirmed cases with a majority of cases from Asia, Europe and U.S.²
- 200+ countries or territories with reported cases
- Breakdown of global supply chains due to travel restrictions
- IMF sees the world economy suffering its worst recession since the Great Depression of 1930

1. COVID-19 likely to shrink global GDP by almost one per cent in 2020, United Nations, 1 April 2020
2. World Health Organisation, Accessed on 15 April 2020



The outbreak and rapid spread of the coronavirus disease (COVID-19) has roiled markets, disrupted supply chains and is threatening the global economy. Organisations around the globe are countering the crisis, but the continuity plans developed by most are proving to be inadequate. This has also compelled organisations to reassess and evolve their strategies. Below are a few key learnings of organisations while managing operations during the crisis.



Business Continuity Management (BCM) function should have right positioning in organisation which enables to liaise across different functions (such as HR, Admin, IT, Communications etc.) for effective co-ordination and optimal usage of resources during crisis situation. Traditionally onus used to be on CRO, CTO, CIO or CISO for ensuring business continuity, which may not be most effective.



Need to have **authoritative source of information** for all employees to ensure **employee safety** during crisis management phase (travel history (personal or official), travel plans, hometown location, current location etc.).



Recovery strategies need to be developed factoring in non-availability of ecosystem providers, unlike traditional BCM approach where it was built on assumption that essential services (cab and rail services) will be available for employee movement or suppliers will be able to operate during contingency.



Having effective **communication management** with employees, customers, health officials, government, regulators through **multiple channels** such as social media, public relationship to reinforce the confidence in the stakeholders.



Information Technology and Cybersecurity functions should be prepared to provide services in **agile manner** to enable alternate service delivery model. **Security controls** play an extremely critical role and should be proactively designed.



Supply chain needs to have effective resilience such that critical services are not disrupted while **contracts** and agreements should incorporate **force majeure clauses** which address events such as pandemic.



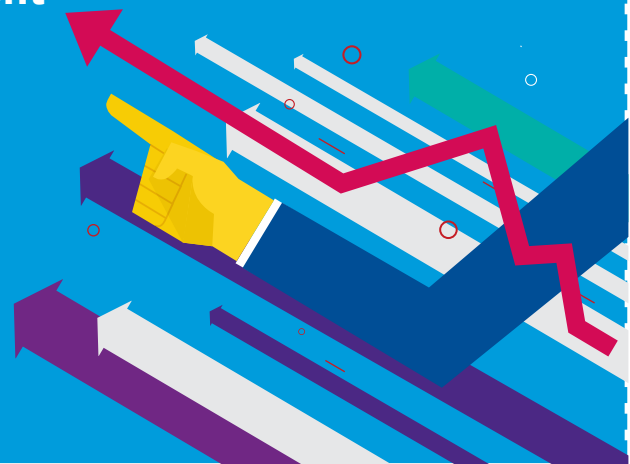
There is a need for enterprises (including brick and mortar enterprises) to effectively use **digital and resilient technology** to continue their operations in pandemic events.

Building operational resilience

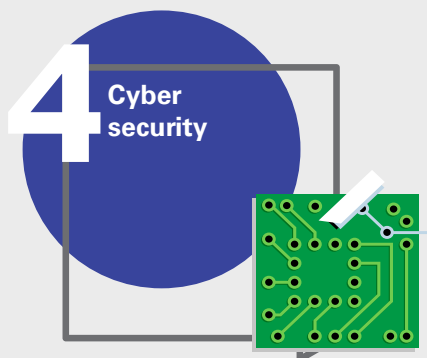
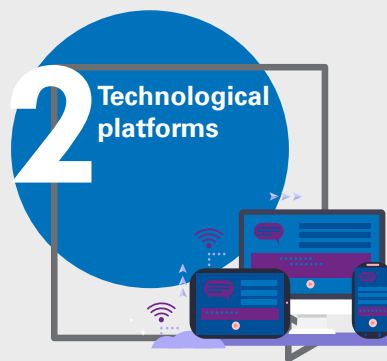
The impact of COVID-19 on customers is profound and the full impact on the economy is still unknown. New habits and behaviours are forming that are likely to continue even after the crisis – and this presents opportunities. In particular, organisations have an opportunity to double-down on digital commerce, expanding existing offerings, creating new lines of service and create an operationally resilient enterprise. Organisations need to define their crisis-management strategies to address long-term and short-term crises differently.

What is an operationally-resilient enterprise?

An enterprise that adapts and flourishes in a changing world has resilient operations that combine agility, flexibility, foresight and robustness as part of its continuity plans.



Pillars of operational resilience



Workforce management

The safety and well-being of the workforce should be the utmost priority for any organisation. To ensure that business requirements are adequately balanced alongside employee needs, enterprises should consider undertaking the required measures on a short and long-term basis.



Challenges

- Individuals need to feel safe, connected, engaged and motivated in order to continue working effectively
- Difficulty in meeting operational needs of business, delivering quality, the changing demands of customers in the face of staff absence and unpredictable availability of workforce
- The need for effective workforce-management capability to optimise resourcing options, including flexible working, contingent and managed service provision.

Short term

- Identify business-critical resources and ensure critical resources within a function are bifurcated into different teams
- Establish a caring culture, i.e. acceptance of WFH realities such as maintain professionalism; set up informal socialising (virtual 'water cooler' or 'tea/coffee chats') etc.
- Understand where demand has fallen or increased and accordingly adjust workload across the workforce.

Long term

- Revisiting the strategy of employee experience design based on the new normal
- Developing a culture of working remotely where people are aware of do's and don'ts of remote working environment
- Shifting from role-based to skill-based organisational design
- Developing a strategy to move resources without impacting operational capabilities
- Reskill and/ or upskill resources to enhance fungibility of resources across different functional capabilities.



Technological platforms

Effective communication and digital channels are essential for ensuring adequate response to a crisis. Organisations have started acknowledging the need to invest in technology and infrastructure to support teleworking and virtual collaboration capabilities.



Challenges

- Adaptation of delivery team to new operating model and changes in tools and technologies being used
- Capacity of collaboration tools and remote-working solutions to cope with exceptional demand driven by remote working
- Using data to rapidly drive insights and reacting quickly to rapid changes while ensuring that sensitive data remains secure and protected
- Lack of flexibility in software licensing contract.

Short term

- Tally information technology priorities with business for rapid adjustment and flexibility
- Ensure that remote working capabilities are scaled up to handle a large number of colleagues who will need to work remotely
- Review helpdesk capacity for responding to queries from users who are unable to login or are unfamiliar with the remote-working environment
- Extending self-service capabilities particularly in password resets, multi-factor authentication management and application provisioning
- Ensure remote monitoring and management capabilities for data centre and technology facilities
- Leverage technologies such as cloud, AI etc. to enable flex capacity planning for information technology service.

Long term

- Evaluate use of robotic process automation (RPA) techniques
- Embed data-driven culture to adapt and provide insights into changing customer needs
- Focus on embedding disaster-recovery playbooks and scenario-planning improvements.
- Review and reprioritise strategic technology investments and accelerate change programmes that actively support resilience
- Recalibrate licensing contract with respect to the demand during crises.
- Evaluating the options for elastic infrastructure and services

B Supply-chain resilience

Most organisations are heavily dependent on suppliers. Supply-chain resilience requires the ability to manage risk such that the organisation is better positioned than its competitors to deal with – and even gain strategic advantage from – disruptions.



Challenges

- Limited understanding of who are the critical suppliers and what critical or niche services they are providing
- Managing high-risk contracts with suppliers/service providers
- Lost revenue and poor customer service due to failure of supply
- Limited time and resources to develop contingency supply options, including cost, timings and manufacturing facilities.

Short term

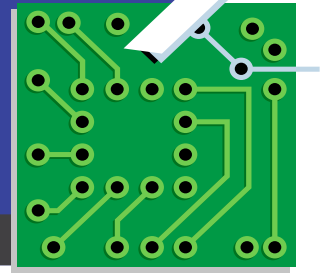
- Communicate and collaborate with critical suppliers and understand their plans to fulfil and prioritise in the face of disruption
- Prioritise your demand and reconfigure global and regional supply-chain flows. Furthermore, take proactive action to address anticipated shortages
- Assess risk factors that may escalate cost and impact service and inventory capabilities
- Recalibrate supplier contract and supply-chain management to develop capability of buffer stock within a defined duration at the time of crises.

Long term

- Restructure supply chains to be more robust, including substituting suppliers
- Move towards flexible contracts and implement multi-sourcing strategies
- Identify activities to be transitioned from external operations back in-house
- Develop a mechanism to proactively monitor the supplier sustainability mechanism and challenges
- Develop a mechanism to bring consumption close to the point of supply or vice versa
- Re-evaluate the sourcing strategies for critical services and supplies.

Cybersecurity

Organised criminal groups are using the fear of the pandemic to carry out highly targeted spear-phishing campaigns and set up fake websites, leading to an increased risk of a cybersecurity incident. Adequate cybersecurity controls should be identified and implemented to mitigate risk associated with pandemic situation.



Challenges

- Understanding the impact of the pandemic on cyber resilience
- Dealing with pandemic-themed cyber threats
- Managing escalating costs of information technology security when budgets are constrained
- Dealing with the reduction in the effectiveness of authorisation and existing security incidents detection processes as a result of widespread remote working.

Short term

- Focus on embedding pragmatic remote-working security controls to deal with pandemic-themed threats
- Ensure preparedness to deal with cyber-attacks, including ransomware
- Ensure security operations teams are able to work remotely and continuously monitor irregular behaviour to prevent fraud
- Review dependency on managed-service providers and seek assurance on security controls for which they are responsible
- Remind employees about disaster-themed phishing attacks.

Long term

- Migrate to a security operation model that allows for greater use of automation
- Test the robustness of established cyber resilience, including response to phishing and ransomware, and enhance it further
- Perform cyber-risk assessment and revisit the cyber-security strategy
- Build zero trust architecture
- Invest in remote SOC monitoring and reporting skills and capabilities.

5 Robust crisis communication

Communication issues can not only impact an organisation's reputation but also have an adverse impact on employee morale. Thus, organisations need a clear and robust crisis communication strategy for responding to any business disruption.



Challenges

- Minimising reputational damage and financial losses
- Communicating decisions and underlying reasons to stakeholders, financiers, regulators and staff
- Identifying a single version of truth since it is easy to lose track of the actions being taken and the decisions that are being made in a fast-changing environment.

Short term

- Determine the person who will communicate to the entire organisation and key decision makers for the organisation's response during the crisis
- Create communications protocols to communicate with customers, suppliers, media, employees and regulators
- Build channels for employees and customers to raise concerns and use social media as a communications channel
- Identify reliable sources of external information for providing insights during the crisis
- Proactively drive lines of communication with employees through email, intranet, chatrooms, etc. to provide reassurance and manage expectations.

Long term

- Establish centralised and robust communication strategy for communicating with customers, employees, suppliers and media
- Basis the lessons learnt, strengthen the existing crisis communication strategy
- Engage regulators and legal team on regulatory-reporting requirements.



Facilities management

Premises and properties are one of the largest and most important business assets. Thus, it is important for organisations to focus on safeguarding their facilities and adapt to changing conditions and maintain or regain functionality.



Challenges

- Meeting health and safety requirements and protecting company assets
- Providing a safe environment for on-site workers and maintenance staff
- Maintaining uninterrupted and back-up power supply
- Ensuring meeting the cleaning requirements of the building during low occupancy
- Visitor management plan to ensure crises management for visitors or temporary employees.

Short term

- Identify facility-related services that are critical to resilience across building types
- In case of a pandemic or epidemic where sites are still occupied, regularly deep clean the public areas
- Ensure sufficient supplies to maintain the health and safety of employees and visitors
- Redesign building occupancy to decongest the building and optimise the contact points
- Assess and enhance the sanitisation capabilities across the facilities.

Long term

- Where facility-related assets have reached the end of their asset life, plan for replacement or renewal
- Assess the ability of facilities management providers to continue service provision during business disruption
- Assess and make changes to your insurance cover to minimise financial disruption in the event of loss or damage of asset
- Design and implement a robust remote building-management system.

Path to the new normal

The collective experience of going through this common crisis will lead to the questioning of fundamental assumptions and priorities, which will create both challenges and opportunities. As the world adjusts to the new normal, organisations need to rethink strategies to drive resilience and emerge from this crisis stronger.

In order to effectively recover from the crisis and embrace the business opportunities that may arise from disruptions caused, organisations should focus on the following critical areas to chart their path in a post COVID-19 world.

Cash is king' for businesses

The COVID-19 crisis has rendered over leveraged companies as the most vulnerable. This situation has reiterated that it is important to be financially prudent and conserve cash.



Push for digital transformation

Even the most brick-and-mortar organisations have been forced to rely on their digital channels. This presents a real and immediate opportunity to drive efficiencies through digital. The crisis has also highlighted the importance of investing in enabling technologies such as cloud, data, artificial intelligence and robotic process automation (RPA).

This will change the way we work with far-reaching implications on B2B, B2C, B2G services, commercial real estate, e-commerce, e-governance, cyber-security, process automation, data analytics, self-service capabilities, etc.



Supply-chain resilience is key

While localisation is a trend we covered earlier, individual companies will want to ensure their supply chains are resilient enough to remain competitive as the risks to supply chains are numerous and continuously evolving.



Increased localisation of sourcing processes

Organisations should reassess sourcing strategies and identify local sourcing partners that may be relied upon, especially for essential services and for sectors that are seen as strategically important.



Building agility

The ongoing pandemic is forcing companies and countries to take quick action in the absence of perfect data while remaining customer centric, addressing employee needs and reinforcing stable team dynamics. Going forward, policies will need to evolve faster than the market and policymakers will need to be more responsive, inclusive and agile.





With the unexpected now, the new normal, companies must strategically rethink their business-continuity plans to remain agile and resilient.

KPMG in India contacts:

Atul Gupta

Partner and Head

IT Advisory

India Cyber Security Leader

T: +91 124 307 4134

E: atulgupta@kpmg.com

Nitin Shah

Partner

IT Advisory - Cyber Security

T: +91 124 336 9062

E: nitinshah@kpmg.com

Merril Cherian

Partner

IT Advisory- Cyber Security

T: +91 80 6833 5524

E: mcherian@kpmg.com

home.kpmg/in



Follow us on:

home.kpmg/in/socialmedia



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 endeavour 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, an Indian Registered 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.

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

This document is meant for e-communication only. (005_THL0420_RU)