# Key success factors for Operational Resilience

July 2020

The coronavirus (COVID-19) continues to have a significant impact on individuals, communities and businesses globally. There are significant challenges that businesses face due to the constantly evolving circumstances. Being able to lead the response confidently and maintain operational resilience is one of them. Effective crisis management and business continuity approaches, focusing on your most important services, creating the leadership structures to enable you to manage your response, and continuing to operate your most critical business functions is key. These approaches rely on continuity in the supply chain, technology and, of course, your people.

Key considerations in determining the focus of your response should include:

- **Finance and reputation:** What is required to continue to generate revenue, what levels of financial loss can be tolerated in the short, medium and long term, and what are the reputational risks that need to be addressed? What incremental cost exposures (e.g. shipping, labour, equipment) will continue to be required?

- **Stakeholders and people:** Who are our key stakeholders and what services are critical to them?

- **Market impact:** Where do we have significant market presence, which of our services are critical to the functioning of our market sectors and how might we be affecting the market – currently and in the future?

- **Regulatory and compliance:** How am I complying with applicable regulations given remote working arrangements?

- **Operational:** How have aspects such as supply chain, customer service and finance been impacted by COVID-19? How are you using this situation to assess opportunities to digitise and automate to improve resilience?
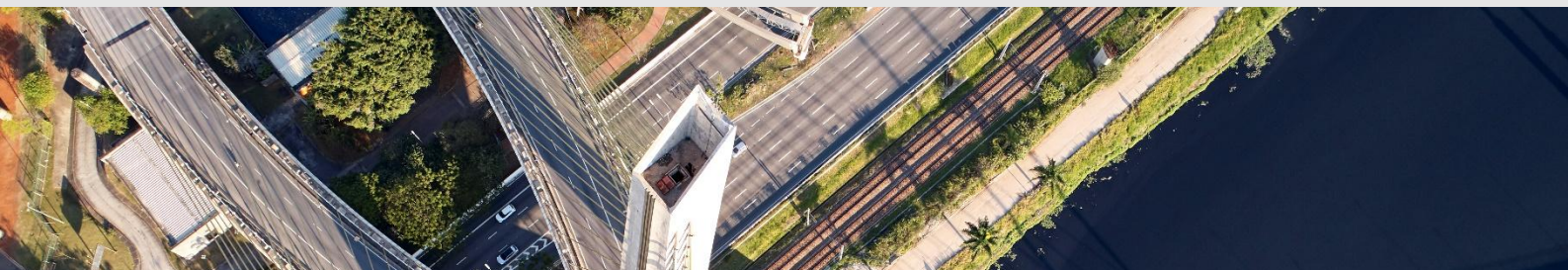
Key Operational Resilience Considerations

Protecting critical services and activities

Identifying and maintaining critical business services, and where to focus efforts under stress

Crisis and Business Continuity Management

Responding and preparing for future crisis and business continuity scenarios

Technology Resilience

Maintaining technology resilience and recovery capability in a high-risk environment

Supply Chain

Challenges for components of the supply chain to implement and operate continuity measures

Workforce and Culture

Enabling your workforce to adapt to new ways of working

Risk and Governance

Managing your 'elevated' and/or 'altered' risk profile within your risk appetite

pwc

Managing disruptions to critical business services

	Short term (4 – 8 weeks) Mobilise*	Medium term (2 – 6 months) Stabilise	Long term (6+ months) Strategise
Protecting Critical Services and Activities Identifying and maintaining critical business services, and where to focus efforts under stress **Identification of critical business services:** At this time, it is important to understand your organisation's end to end business services (that may span across multiple business units) and prioritise these services based on criticality, both to the organisation and to customers. It will also be important to identify the necessary resources (people, process, technology, facilities and information) that support the delivery of these critical business services. Organisations should also identify where resources are provided by an intra-group function or external third party. **Setting and operating within impact tolerances:** Organisations should look to understand the maximum tolerable level of disruption to their critical business services, including the maximum tolerable duration. These should be scenario tested to assess your organisation's ability to manage service delivery within impact tolerances in varying scenarios.	• Assess the impact to critical business services and activities, and prioritise effort to address effectively	• Mapping of end to end business processes, overlaying key supporting resources, and assessment of criticality • Identify and assess 'Single Points of Failure' (SPOF) for critical services • Set impact tolerances for your most critical business services and planning for scenario testing	• Conduct testing to identify weaknesses in resilience procedures that are unable to be managed within the impact tolerance limits set. Develop remediation plans, or agree to risk accept
Crisis and Business Continuity Management Responding and preparing for future crisis and business continuity scenarios **Fit for purpose crisis management and business continuity plans:** In light of COVID-19, it is expected that organisations review and ensure that their resilience procedures remain fit for purpose during a pandemic. It will be important to understand the current environment and plan for future impacts on local and international market operations, supply chains, cash flow and workforces. Different scenarios should be considered and the latest WHO and government guidelines be considered in planning and key decisions. These scenarios should then be stress tested to enable weaknesses to be identified and appropriate safeguards to be implemented. **Agile, aligned and effective communications:** Stakeholder management will be paramount during these uncertain times. This will apply both to internal and external communications - it will be key to manage customer expectations and work with suppliers to keep them up to date with the evolving situation. This may be supported by collaborating with government agencies in managing your response to this crisis.	• Review existing arrangements, establish a COVID-19 planning team, determine reasonable worst-case scenarios (RWCS) and implement response processes	• Understand the current environment and plan for future impacts on local and international market operations, supply chains, cash flow and workforces • Review and update business resilience documents, including incorporating learnings into your pandemic plan	• Consider the automation of resilience processes to enable flexibility with business change, reduce dependence on people to act, and improve alignment and consistency between plans • Plan for more frequent business continuity, crisis management and disaster recovery plan tests to identify weaknesses and gaps
Technology Resilience Maintaining technology resilience and recovery capability in a high-risk environment **IT service dependencies and priorities:** The COVID-19 response has shown the need for have a clear view of all technology assets required, and their interdependencies, to deliver an IT service. Critical IT capabilities should be stress tested to prepare for the additional strains resulting from the increased use of online platforms and new working arrangements. Existing scenarios such as loss of internet access should be re-evaluated for the current situation to ensure that plans are still fit for purpose given the current operating model. **Automation and digitisation agenda:** There may be an opportunity to uplift your organisations digital capabilities to optimise operations, improve security posture and support new working arrangements where these were not possible previously. This may help to relieve the pressure on staff, streamline processes and reduce cost.	• Establish capacity, demand and capability for remote access, then test and implement solutions • Review performance, capacity and scalability requirements to ensure the technology is able to withstand extreme loads	• Update existing, and development of new IT service continuity plans for disruption scenarios not considered previously • Assess the resilience of your technology environment supporting critical business operations	• Consider digitisation of existing manual processes to improve resilience, support new ways of working and also support future efficiencies

Whilst the short term impacts have been felt, it is still prudent to check that these activities have been considered for your environment

Managing disruptions to critical business services

	Short term (4 – 8 weeks) Mobilise	Medium term (2 – 6 months) Stabilise	Long term (6+ months) Strategise
Supply Chain — Challenges for components of the supply chain to implement and operate continuity measures **Coordinated approach with third parties**: Collaboration with critical third-parties may help to develop a coordinated approach to dealing with service disruptions. Organisations should regularly monitor their third parties via contractually agreed Service Level Agreements (SLAs). These metrics and regular conversation with third parties may highlight potential weaknesses in their supply chains (third and fourth parties), and if there are any planned alternatives to obtaining critical services and supplies if the increased demand cannot be met. Logistical disruptions to the supply chain should also be considered and if any contingency measures can be implemented.	• Engage with key parties that are part of your supply chain ecosystem, and understand impacts to both upstream and downstream third parties	• Identify if there are any third parties that are no longer required, where activities can be automated or insourced • Assess and re-validate contract clauses including clauses related to 'Force majeure' invocation	• Establish transparency in your third parties resilience processes, policies and frameworks • Re-assess any offshoring models and consider alternatives such as near-shore / on-shoring to have increased control over critical operations
Workforce and Culture — Enabling your workforce to adapt to new ways of working and driving a greater operationally resilient culture **Improving workforce operation and productivity:** Amid the business slowdown, there is an opportunity to upskill / cross skill staff to enable more agile teams, and improve workforce capability and productivity. Leveraging productivity tools and digitising previously manual tasks may help to improve the efficiency of your workforce. Health and wellbeing of staff should also be considered as this may have a knock on impact on productivity and staff engagement. As the pandemic restrictions lift, organisations should consider the impact of multi modes of operation as some workforces remain remote and others not, and how critical business services will be delivered. **Operational resilience culture:** It is important to start considering, and if not already done so, implementing an operationally resilient culture that will help to ensure that resilience is front of mind. There should be a goal to sustain this at all grades going forward and have the appropriate endorsement from senior management.	• Re-evaluate available talent and resource pools, and assess whether reallocation may be required for services that are in higher demand • Plan for the multi modes of operation required as restrictions lift, and how critical business services will be delivered	• Re-assess the productivity of your virtual working arrangements and adopt new working practices and technologies to maximise productivity • Offer digital upskilling / training to improve productivity • Review the operational resilience culture of the organisation and implement measures to improve this	• Review and redesign your organisation structures so as to maximise productivity and agility as well as reduce cost • Reconsider and optimise workflows, decision-making rights and work processes, considering the adoption of automation and AI to reduce workforce requirement
Risk and Governance — Managing your 'elevated' and/or 'altered' risk profile within your risk appetite **Impact to operational risk profile:** The response to COVID-19 has seen a number of organisations implement business changes, which which may have increased or introduced additional risks which will need to be mitigated. Organisations may need to reassess changes to the environment to determine whether sufficient controls are in place, and evaluate what processes and controls will continue to be required or changed in the mid to long term, and whether they are within risk appetite. **Critical role of risk functions:** The role of the three lines of defence will be key to support the implementation, or to conduct reviews over material changes in the environment, assess potential impacts to the organisation's risk profile, and to validate the ongoing effectiveness of key controls. **Governance:** There should be a robust governance framework in place to monitor resilience across the organisation. This should include the appropriate governance forums, policies, standards, reporting and measurement.	• As changes are required to respond to COVID-19, the impact to the control environment and risk profile should be assessed prior to implementation	• Assess the revised control environment to determine sufficiency of design, and operating effectiveness of controls • Increase scrutiny and oversight by the board on resilience processes. There should also be greater accountability and ownership for resilience by executives and management	• Review and uplift risk management processes, functions and culture for readiness to support new working arrangements • Review and agree your organisation's risk appetite • Implement a governance framework for resilience that can be sustained in the future

We can work alongside you to tackle the challenges you face in responding to COVID-19

Operational resilience reviews and capability uplift

We bring expertise in responding to disruptive scenarios, derived from real-world experience with our client base, that can help with your COVID-19 response and recovery. This includes conducting operational resilience assessments and the uplift of capability across the six core operational resilience domains to support continuity of critical business services. Some additional services we can support you with include:

Critical services and activities
- Identifying or reviewing your critical business services, including the resources (people, process, technology, facilities and third parties) supporting these services
- Assessing the resiliency of your critical business services, including the review of single points of failure (SPOF)
- Assessing, or supporting the establishment of your impact tolerances and scenario planning activities

Crisis and business continuity management
- Reviewing and/or facilitating documentation of Business Impact Assessments, Business Continuity, Crisis Management, Pandemic and Disaster Recovery Plans
- Scenario testing and walkthroughs of your business resilience plans
- Supporting the development of a communications plan and strategy during a crisis

Technology resilience
- Reviewing IT critical processes to assess and benchmark maturity and resilience of processes
- Reviewing critical IT services for the resiliency of technology architecture, including review of single points of failure (SPOFs)
- Assessing your environment for opportunities to improve resilience through reducing manual business processing and increasing the use of automation or digital solutions

Supply chain
- Independent review of critical third parties, such as key manufacturers and logistics services (particularly exit management plans and Business Continuity Plans)
- Assessing concentration risk across your supply chain, including potential offshore impacts
- Reviewing and uplifting third party governance frameworks, policies and processes

Workforce and culture
- Planning of resource roadmaps and solution planning for workplace adaptation based on multi-scenario impacts
- Reviewing usage of tools to drive improved productivity across the workforce. Assessing use of unsanctioned tools through cloud discovery reviews
- Assessing workforce culture and remediation activities

Risk and governance
- Reviewing your revised control environment to determine the sufficiency of design, and operating effectiveness of controls
- Assessing your risk operating model – including governance, processes, technology and risk culture
- Reviewing or developing your organisation risk appetite

Client case studies

Large Australian and NZ Retail Firm

We were engaged to support the refresh of this organisation's business resilience documents, including business continuity, incident and security standards. With the evolving COVID-19 situation, we also supported the re-development of their crisis management and pandemic plans, to align to the appropriate government health guidance, industry good practice, and incorporate learnings from the current pandemic. These documents have formed the foundations for this organisations' business resilience practices, with the aim for these to be digitised in the near future.

Large Australian Financial Services Firm

Due to COVID-19, offshore suppliers and BPO providers were impacted due to insufficient business continuity procedures to support remote working. This led to an inability to continue critical back office processing activities for the client. Our onshore service delivery teams were quickly mobilised and were able to be embedded within their business and continue their processing activities. Based on our previous knowledge of their environment, we are supporting them drive their digitisation and automation agenda to make processes more efficient.

Contents

Ryan Ettridge | Brisbane
Partner
M: +61 417 702 234
E: ryan.ettridge@pwc.com

Nicola Nicol | Melbourne
Partner
M: +61 436 444 949
E: nicola.nicol@pwc.com

Craig Sydney | Sydney
Partner
M: +61 400 215 757
E: craig.sydney@pwc.com

Shad Sears | Canberra
Partner
M: +61 419 771 079
E: shad.sears@pwc.com

Jason Knott | Perth
Partner
M: +61 417 455 074
E: jason.knott@pwc.com

Kim Cheater | Adelaide
Partner
M: +61 414 227 035
E: kim.cheater@pwc.com

To find out how PwC Australia is responding to COVID-19, please visit:
https://www.pwc.com.au/about-us/notices/coronavirus.html

For our latest insights and resources, please visit:
https://www.pwc.com.au/important-problems/coronavirus-covid-19.html