Operational Resilience

The evolution of Business Continuity Management and Disaster Recovery
Increasing market uncertainty, dependence on third parties and complex IT systems and processes have made disruptions more likely and their impact potentially more severe. Such disruptions make operational resilience a key regulatory priority for supervisory authorities such as APRA (as set out in their supervisory priorities for 2022) but also a key priority across a wider range of industries, particularly following the implementation of the Critical Infrastructure Resilience Strategy by the Department of Home Affairs.

What is it?

Operational resilience is now a key priority for financial services regulators and the Department of Home Affairs. APRA has noted this as one of its key supervisory priorities for the year ahead whilst the Department of Home Affairs has implemented its own Critical Infrastructure Resilience Strategy that aims to ensure the continued operation of critical infrastructure in the face of all hazards.

Traditional approaches to managing disruption through business continuity management and disaster recovery have focused on assets in siloes instead of critical components of end to end service delivery. Traditional approaches have also been retrospective in nature, whereas operational resilience will seek to ensure that any disruption is prevented in the first place.

Regulatory guidance from APRA is still pending, however it’s likely to require firms to prevent disruption occurring to the extent practicable; adapt systems and processes to continue to provide services and functions in the event of an incident; return to normal running promptly when a disruption is over; and learn and evolve from both incidents and near misses.

To comply with operational resilience requirements, firms will need to ensure that important business services (IBS) are identified with appropriate tolerances, the firm’s ability to remain within its impact tolerance for each IBS is tested and updates are made to governance, operational risk management, business continuity planning and the management of outsourced relationships.
Why is it important?
Financial services firms have more dependencies on service delivery than ever before and the risk of disruption has only intensified in recent years with the adoption of digital solutions and the increasing use of outsourced service providers.

As firms continue to develop business services to meet growing customer expectations the need to adapt and accelerate the pace of this change increases the risk of disruption, particularly to IT related capabilities which are increasingly susceptible to more sophisticated cyber and ransomware attacks.

In addition, firms have been trying to manage a significantly different operating environment as a result of the global pandemic, fundamentally changing the way they interact with technology, customers and their own employees. Climate change is also set to test resilience to physical risks and disrupt operations through changes in market sentiment and economic models.

All of this makes operational resilience even more important as firms not only seek to prevent disruption but also adapt to it.

Who is this important for?
Resilience is a collective commercial imperative that should be considered by all. Firms must seek to transform and strengthen their resilience to disruption, incidents, and attacks across technology, data, third parties, facilities, operations, and people.

Given all of these issues have the potential to impact almost any area of a firm, it's important that operational resilience is viewed as an enterprise wide requirement, rather than something that should be managed in one area.

Accountability rests with boards and senior management to provide effective challenge of their organization’s resilience and residual risks that remain relevant to their operations.

Firms that manage to effectively address operational resilience will be able to unlock significant benefits, including reduction in operational costs, reduced complexity in service delivery, more efficient innovation programs and a better customer experience.
Operational Resilience together with business continuity management (BCM) and disaster recovery (DR) ensures that firms can prepare, resolve and recover from disruptive incidents. Operational Resilience builds on BCM and DR to increase the focus on anticipation, prevention and adaptation to disruption.

Operational resilience represents a natural progression from BCM and DR as financial services firms continue to expand service offerings, rely on complex system architectures and depend on third parties for the delivery of important business services.

The table to the right illustrates the progression from BCM/DR to operational resilience across six key areas.
In what areas can PwC help?

PwC bring expertise in responding to disruptive scenarios and implementing regulatory requirements for operational resilience derived from real-world experience working with international regulators and our client base. This includes conducting operational resilience assessments and the uplift of capability across four key areas to support continuity of critical and important business services.

**Governance**
- Define your strategy for operational resilience.
- Review and/or design documentation for Business Impact Assessments, Business Continuity, Crisis Management, Pandemic and Disaster Recovery Plans.
- Support board awareness and senior management preparedness, including assigning roles and responsibilities across the three lines of defence.
- Identify and design operational resilience reporting to ensure that the most appropriate data is being tracked and analysed at the correct level.

**Target Operating Model**
- Integration of operational resilience into operating model design, reflecting changing customer and employee preferences, location strategies, new technologies and economic imperatives that have emerged since the pandemic.
- Independent review of critical third parties to ensure that arrangements are consistent with operational resilience requirements.
- Assess concentration risk across your supply chain, including potential offshore impacts.
- Assess your environment for opportunities to improve resilience through reducing manual business processing and increasing the use of automation or digital solutions.

**Important Business Services Lifecycle**
- Identify and review your important business services, including the resources (people, process, technology, facilities and third parties) supporting these services.
- Assess the resiliency of your important business services, including the review of single points of failure.
- Assess, or support the establishment of your IBS impact tolerances and scenario planning activities.
- Establish quantitative impact tolerances for IBS.
- Review impact tolerances following changes to strategy, customer expectations, technology advances and regulatory change.
- Assist with your resolution planning for an orderly market exit in the event that the resilience of important business services cannot be sustained.

**Risk Assurance**
- Review your control environment to determine the sufficiency of design, and operating effectiveness of controls in response to disruptive scenarios.
- Assess your risk operating model – including governance, processes, technology and risk culture.
- Review your risk appetite for disruptive scenarios, including the design and collation of metrics and reporting.
- Assess compliance against any upcoming regulatory requirements.
Contact us

Peter Malan
Partner
Cybersecurity & Digital Trust
+61 413 745 343
peter.malan@pwc.com

Susanna Chan
Director
Cybersecurity & Privacy
+61 414 544 066
susanna.chan@pwc.com

Sarah Hofman
Partner
Risk & Regulation
+61 403 068 645
sarah.hofman@pwc.com

Daniel Harb
Director
Banking & Capital Markets
+61 433 099 889
daniel.harb@pwc.com

Jon McNish
Director
Organisational Resilience
+61 478 651 777
jon.mcnish@pwc.com

Noel Williams
Partner
Cybersecurity & Digital Trust
+61 416 661 332
noel.williams@pwc.com

Sam Hinchcliffe
Partner
Banking & Capital Markets
+61 434 182 665
sam.hinchcliffe@pwc.com

Bernadette D‘Alessandro
Partner
Risk & Regulation
+61 414 716 126
bernadette.b.dalessandro@pwc.com

Sean Conley
Senior Manager
Risk & regulation
+61 481 930 953
sean.a.conley@pwc.com

pwc.com

© 2022 PricewaterhouseCoopers. All rights reserved. PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Liability limited by a scheme approved under Professional Standards Legislation. At PwC Australia, our purpose is to build trust in society and solve important problems. Find out more and tell us what matters to you by visiting us at www.pwc.com.au

PWC200394452