

Operational Resilience: Insurance in focus

Prudential Standard CPS 230

March 2023

Operational Resilience

APRA's take on Operational Resilience

In an environment where change is constant, risk management and broader resilience capabilities need to quickly adapt to support business agility. APRA's proposed Prudential Standard CPS 230 Operational Risk Management (CPS 230), is designed to enable this, setting out key requirements for managing operational risk, including replacing the business continuity and service provider management standards (CPS 232 Business Continuity Management and CPS 231 Outsourcing) with updated requirements.

Operational risk management will be key, alongside the existing Prudential Standard CPS 234 (Information Security), in driving APRA's desired outcome to improve operational resilience and minimise the impact of disruption to customers and the financial system.








Embracing risk in the face of disruption

Insurance entities are navigating a new and volatile market, faced with known and emerging risks. Many are still adjusting to 'COVID-normal,' where business models have been challenged, and in some cases reinvented. Further uncertainty has been presented through continuous supply chain disruptions, accelerating digital and technology adoption, heightened cyber security and data risks, as well as severe weather conditions. The latter for example, has placed significant strain on insurance companies to deliver timely and appropriate outcomes to their customers due to increased claims volumes, longer claims processing timelines, critical shortages in service providers and materials, and increasing costs.

Insurers are increasingly relying on service providers, particularly as they transform processes such as claims management, to exploit new technologies, increase collaboration, enhance customer experience and drive efficiencies. As these supply chains become more complex, including the reliance on third, fourth parties and beyond, the downstream impacts of service providers could cause intolerable harm to customers.

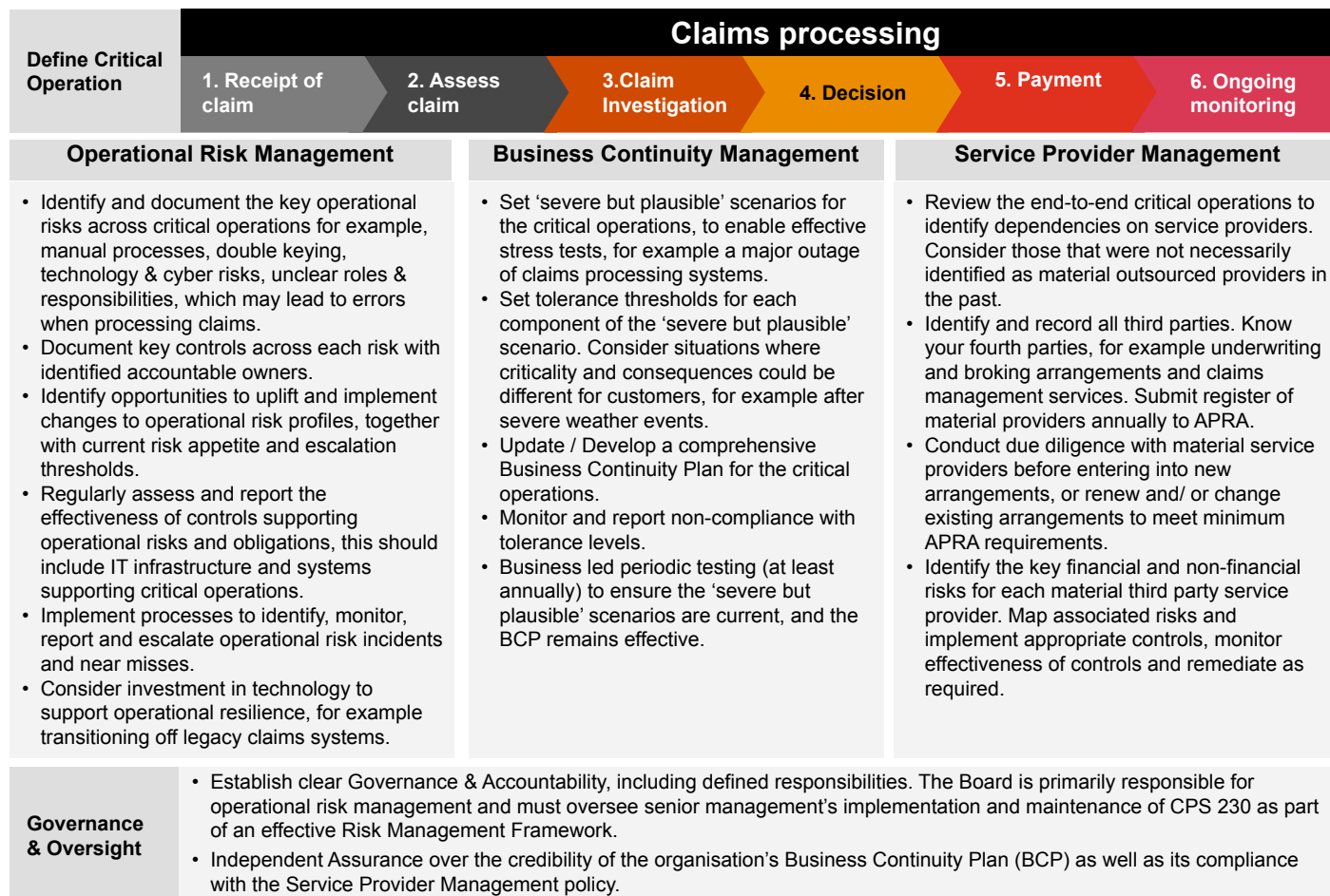
As insurers embark on the CPS 230 journey, it is important that the requirements are not considered in silos and it is critical that Board accountabilities are supplemented with clearly delegated responsibilities across the organisation to support comprehensive end-to-end mapping of critical operations to inform an appropriate response. With the interconnectedness of other regulatory requirements such as the introduction of Financial Accountability Regime (FAR), there is also opportunity to leverage foundational principles in the enhanced decision making process and the new Board accountabilities required by CPS 230. Importantly, getting this right now means mapping and implementing an effective enterprise wide controls framework which mitigates the suite of operational risks.

What do insurers need to do?

 <p>Increase Board & senior management accountability</p>	 <p>Identify critical operations</p>	 <p>New operational risk management requirements</p>	 <p>Set impact tolerances & perform scenario testing</p>	 <p>Determine Material Service Providers (MSPs)</p>
<p>The Board is ultimately accountable for operational risk management and must oversee senior management's implementation and maintenance of CPS 230.</p> <p>Under the new standard, this includes overseeing the effectiveness of key internal controls and approving tolerance levels for critical operations.</p> <p>The Board must approve the service provider management policy and supervise the performance of service providers.</p>	<p>To support a comprehensive Operational Risk Profile and Business Continuity Plan (BCP), Entities must understand and maintain their critical operations to minimise the likelihood and impact of disruption to these as part of their business continuity planning.</p> <p>This includes identifying and considering the interdependencies that can be impacted during disruption (including systems, infrastructure, people and service providers).</p>	<p>Entities must manage their full range of operational risks by maintaining an Operational Risk Profile, supported by a comprehensive assessment.</p> <p>This includes the implementation of internal controls to mitigate these risks within appetite, which should be embedded and regularly tested.</p> <p>Entities must also maintain a strong data and IT infrastructure to meet business requirements and support critical operations.</p>	<p>Entities must establish Board-approved tolerances for the maximum level of disruption they are willing to accept, including around data loss. Impact tolerance levels set need to be customer and outcomes-focused.</p> <p>Entities are expected to maintain critical operations within tolerance levels and conduct regular scenario testing to calibrate impact tolerances.</p>	<p>Entities must understand and manage the risks associated with the use of the service providers that support their critical operations or expose them to material operational risk, including downstream providers (fourth parties).</p> <p>A register of MSPs and associated risks must be reported to APRA annually, as well as changes to MSP agreements.</p>

CPS 230 in practice: Claims processing

To support a comprehensive **Operational Risk Profile** and an appropriate corresponding **Business Continuity Plan**, the Board must understand critical operations across the organisation. This is supported by a detailed end-to-end mapping of each critical operation including their enablers such as technology and material third party **Service Providers**. The identification and implementation of effective key controls which support the appropriate management of operational risk is key in this process. The below illustration summarises the key CPS 230 requirements across “**Claims Processing**” as a critical operation.



How can we help?

Set up the right foundation	Increase Board & senior management accountability	Identify critical operations	New operational risk management requirements	Set impact tolerances & perform scenario testing	Determine Material Service Providers (MSPs)
<ul style="list-style-type: none"> CPS 230 readiness review, maturity and benchmarking assessment Operational resilience Target Operating Model (TOM) design Operational resilience program planning, scoping and delivery 	<ul style="list-style-type: none"> Operational resilience governance and accountabilities definition Board and executive awareness sessions 	<ul style="list-style-type: none"> Critical operations definition and documentation, including resources Internal controls mapping, across the identified risks and obligations 	<ul style="list-style-type: none"> Operational risk profiling (incl. risk appetite definition) Operational resilience review to identify potential resilience gaps in the environment Controls assurance (incl. gap identification and remediation action) 	<ul style="list-style-type: none"> Impact tolerance identification Business Continuity and Disaster Recovery Planning Training and awareness Scenario testing 	<ul style="list-style-type: none"> Material service provider (MSP) assessments Third Party Risk Management Framework Third party controls testing (for MSPs)

Contacts

Please reach out to any of the following members of the operational resilience working group, should you wish to obtain further information.



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



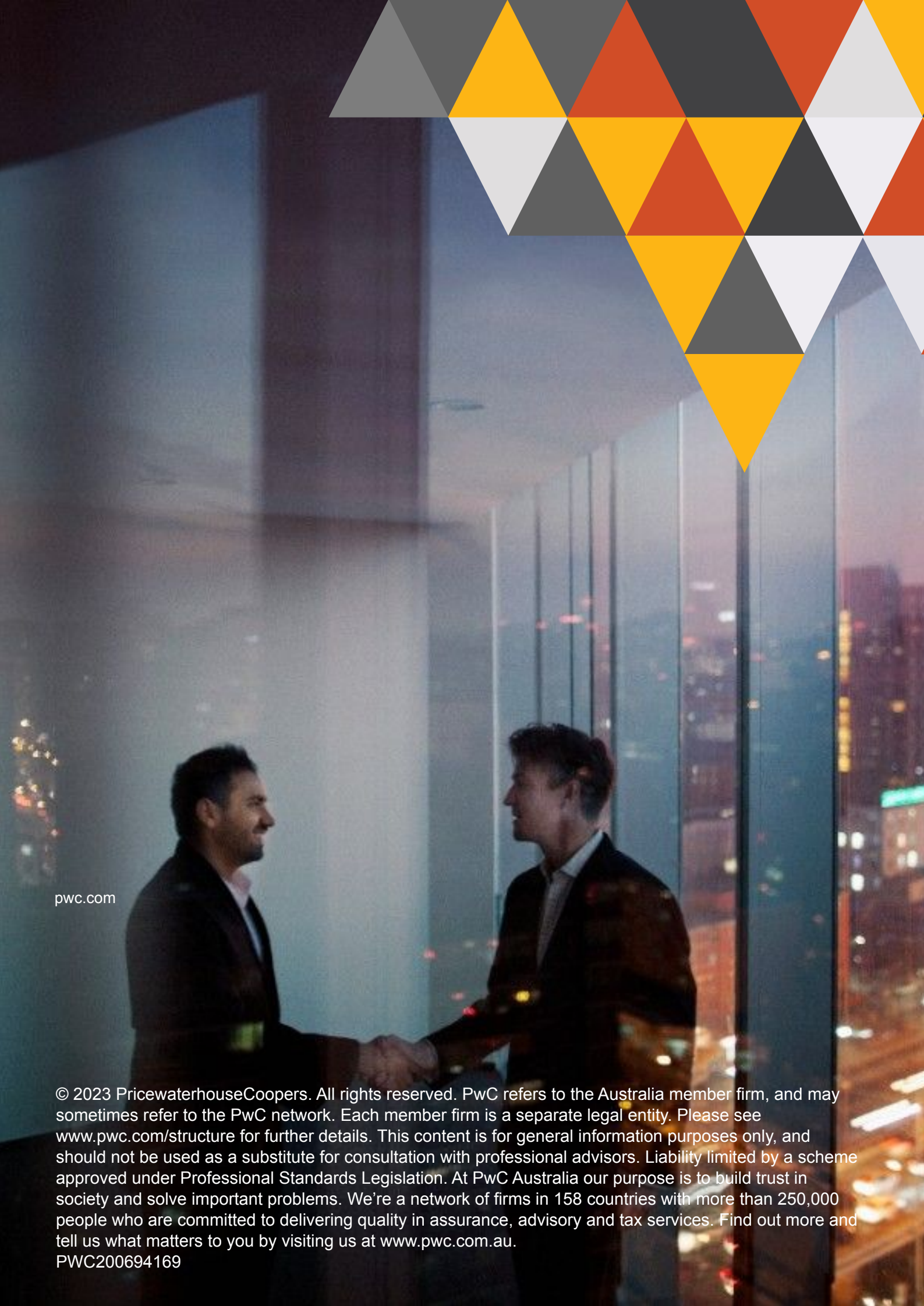

Sam Hinchliffe
Partner
Risk & Regulations
T: +61 434 182 665
E: sam.hinchliffe@pwc.com



Susanna Chan
Partner
Operational Resilience
T: +61 414 544 066
E: susanna.chan@pwc.com



Scott Fergusson
Partner
Insurance
T: +61 408 113 914
E: scott.k.fergusson@pwc.com



pwc.com

© 2023 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. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.
PWC200694169