

Operational Resilience: Super in focus

Prudential Standard CPS 230

July 2023



pwc

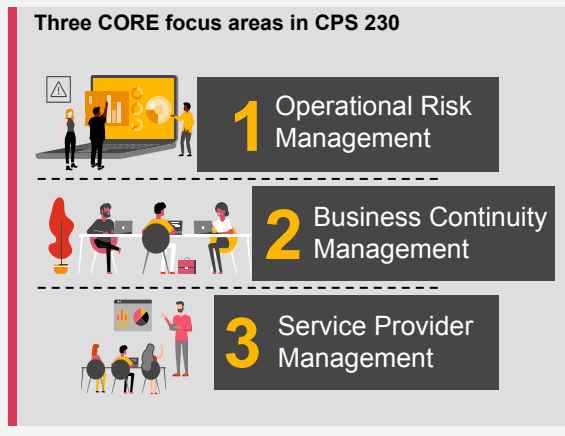
Operational Resilience



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 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. The new standard has an **effective date 1 July 2025** (with existing service provider arrangements getting an extra year until 1 July 2026 to compile).

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 members and the financial system.



Consolidation can create operational risk for super funds






Australian superannuation institutions are undergoing consolidation due to pressures on performance, fees and sustainability. This pressure is also felt by their service providers who themselves have also consolidated in key areas such as administration, custody and insurance as they seek to scale, reduce costs and to meet the needs of superannuation funds.

Consolidation can lead to concentration risk and transition risk as providers exit the market (e.g. in Custody, Insurance and Administration). If not appropriately understood and managed (especially for critical operations) this can cause an intolerable level of harm to members, the viability of the fund and/ or the stability of the superannuation sector.

To succeed on the CPS 230 journey, it is important that the requirements are not considered in silos and board accountabilities are supplemented with clearly delegated responsibilities to support a comprehensive end-to-end mapping of critical operations. With the interconnectedness of other future regulatory requirements such as the Financial Accountability Regime (FAR), Operational Risk Financial Requirement (consultation on SPS 114), Recovery and exit planning (CPS 190), member outcomes and transfer planning, superannuation funds should ensure the approach is consistent and integrated.

Getting this right requires mapping and implementing an effective enterprise wide controls framework to mitigate the suite of operational risks.

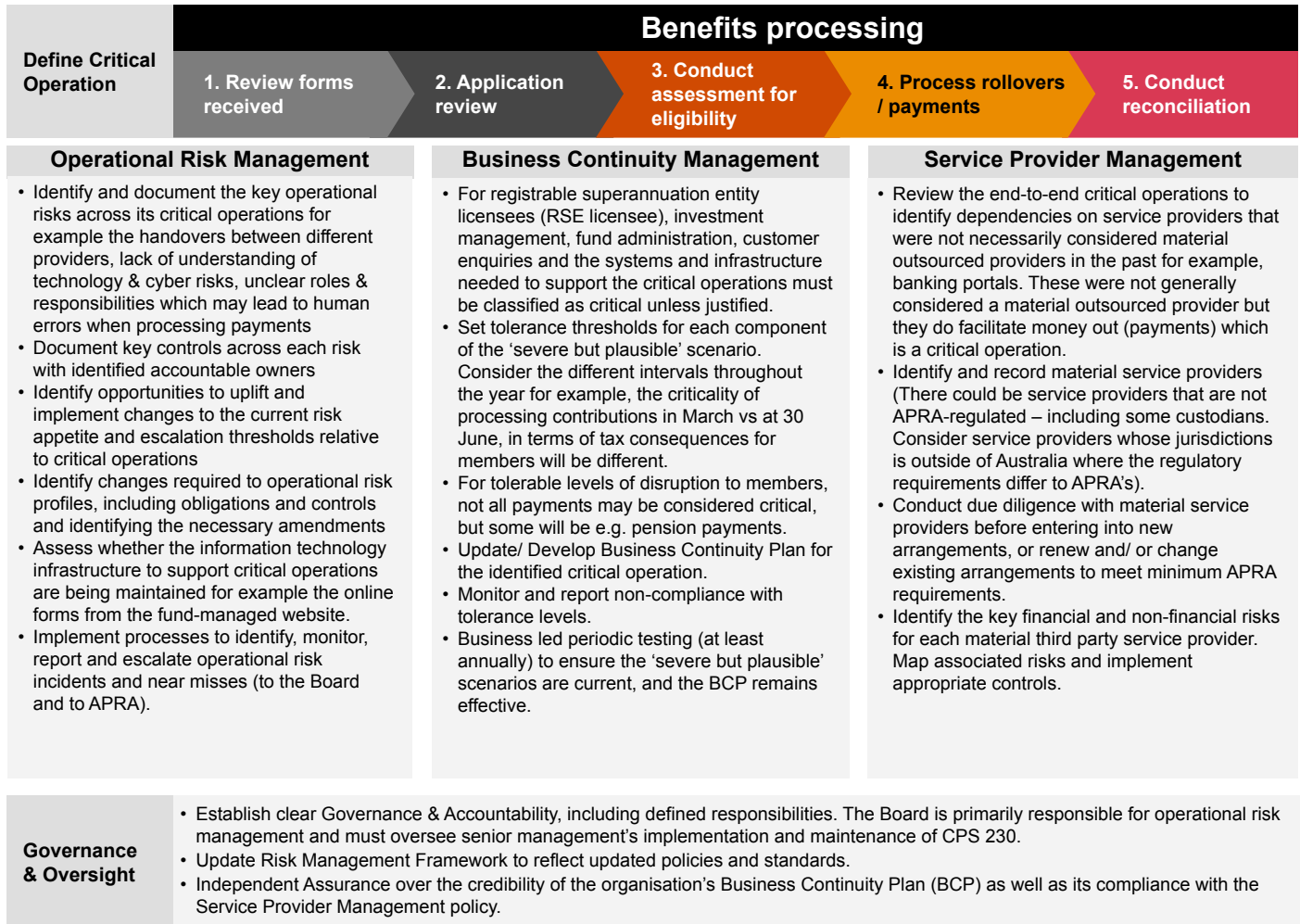
What do funds need to do?

 <p>Increase Board & senior management accountability</p>	 <p>Identify critical operations</p>	 <p>Operational Risk Management</p> <p>New operational risk management requirements</p>	 <p>Business continuity management</p> <p>Set impact tolerances & perform scenario testing</p>	 <p>Service provider management</p> <p>Determine Material Service Providers (MSPs)</p>
<p>The Board is responsible for operational risk management and oversees management's implementation and maintenance of CPS 230.</p> <p>This includes 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 their critical operations and minimise the likelihood and impact of disruption as part of their business continuity planning.</p> <p>This includes identifying the resources and interdependencies that can be disrupted (e.g. people, technology, information, facilities and service providers).</p>	<p>Entities must review and update (where applicable) its Operational Risk Profile.</p> <p>This includes the implementation of internal controls to mitigate risks within appetite and meet obligations, which should be embedded and regularly tested.</p> <p>Entities must also maintain a strong data and IT infrastructure information assets 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 member 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: Benefits 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 considerations for superannuation funds by using “**Benefits processing**” as an example.



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 (incl. framework development) and accountabilities identification 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 update) 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)

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

Contacts	 <p>Peter Malan Partner Cybersecurity & Digital Trust T: +61 413 745 343 E: peter.malan@au.pwc.com</p>	 <p>Carley Bryce Partner Risk & Controls T: +61 412 929 373 E: carley.bryce@au.pwc.com</p>	 <p>Nathan Bonarius Partner Superannuation T: +61 487 887 474 E: nathan.bonarius@au.pwc.com</p>	 <p>Susanna Chan Partner Operational Resilience T: +61 414 544 066 E: susanna.chan@au.pwc.com</p>
-----------------	--	--	---	---



Thank you

[pwc.com](https://www.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