Operational Resilience: Banking in focus

Prudential Standard CPS 230

June 2024

pwc

www.pwc.com

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.

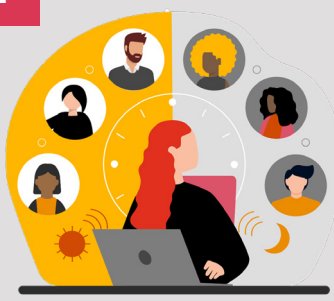
Operational risk management will be key, alongside the existing Prudential Standard CPS 234 (Information Security), in driving APRA's desired outcome to improve operational resilience and minimise the impact of disruption to customers and the financial system.

Three CORE focus areas of CPS 230

1

Operational Risk Management

2



Business Continuity Management

3

Service Provider Management

Embracing risk in the face of disruption

Against a backdrop inflationary pressures and interest rate hikes, Australian banking institutions are navigating a new and volatile market, with known and emerging risks. If not appropriately understood and managed in the context of critical operations (and the ultimate customer impacts when things go wrong), these risks could have far-reaching implications across the organisation and put brand and reputation at stake. Banking products and services have high volumes of customers that are transaction heavy which makes operational resilience so important in this space.

Typically, we are seeing that the banking sector has a more advanced approach to operational resilience, with working groups established to ensure compliance with the new standard. Driving this is the appreciation for how private data and technology incidents have disrupted this sector in recent years, and the regulatory scrutiny that has accompanied these disruptions. In an increasingly competitive market, firms also recognise there is a commercial advantage in developing resilience across their organisation, and the subsequent benefits this delivers in managing risk and continuing to service their customer base.

As banking institutions 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 a comprehensive end-to-end mapping of critical operations to inform an appropriate response. With the interconnectedness of other regulatory requirements such as the Financial Accountability Regime (FAR) (which will replace the existing Banking Executive Accountability Regime (BEAR)), 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 organisations need to do?

Increase Board and senior management accountability

- The Board is ultimately accountable for operational risk management and oversees management's implementation and maintenance of CPS 230.
- This includes internal controls and approving tolerance levels for critical operations.
- The Board must approve the service provider management policy and supervise the performance of service providers.

Identify critical operations

- 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.
- This includes identifying the resources and interdependencies (linked to critical operations) that can be disrupted (e.g. people, technology, information, facilities and service providers), and associated risks, obligations and controls.

Operational Risk Management

New operational risk management requirements

- Entities must review and update (where applicable) its Operational Risk Profile. Organisations will be required to consider this with a critical operations lens.
- This includes the implementation of internal controls to mitigate any identified risks, ensuring that risks remain within appetite, ensuring that obligations are met, embedded and regularly tested.
- Entities must also maintain a strong data and information assets to meet business requirements and support critical operations.
- Incidents (including near misses) will need to be notified to APRA in a timely manner.

Business continuity management

Set impact tolerances and perform scenario testing

- Entities must establish Board-approved tolerances for the maximum level of disruption they are willing to accept, including around time, data loss and minimum service levels they will operate under disruption. Tolerance levels set need to be customer and outcomes-focused.
- Entities are expected to maintain critical operations within tolerance levels and conduct regular scenario testing to calibrate tolerance levels.

Service provider management

Determine Material Service Providers (MSPs)

- 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).
- A register of MSPs and associated risks must be reported to APRA annually, as well as changes to MSP agreements.

CPS 230 in practice:

Mortgage Origination

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 **'Mortgage Origination'** as a critical operation.

Critical Operations for ADIs	The Standard has identified the following critical operations for ADIs (unless justified otherwise): Payments, deposit-taking and management, custody, settlements, clearing, customer enquiries and the systems and infrastructure needed to support critical operations.

Define Critical Operation

Mortgage Origination

1 **Customer inquiry** → 2 **Customer application** → 3 **Application review** → 4 **Credit assessment** → 5 **Decision** → 6 **Ongoing monitoring**

Operational Risk Management

- Define end-end processes for critical operations at a high level, including identifying and mapping resources and assets required to operate critical operations.
- Identify and map the associated obligations, risks (e.g. regulatory risk, technology risk) and controls in place to mitigate risks for business processes, including end-end processes for critical operations.
- Regularly assess and report the effectiveness of internal controls supporting operational risks and obligations including any remediation activities.
- Implement robust processes for identifying, monitoring, reporting and escalating operational risk incidents and near misses (to the Board and to APRA).
- Uplift Operational Risk Profile using a critical operations lens.
- Provide regular updates on the operational risk profile to the Board.

Business Continuity Management

- Once critical operations have been mapped, establish Board approved tolerance levels for critical operations to meet CPS 230 requirements.
- Develop a library of severe but plausible' scenarios for the critical operations, to test ability to operate within tolerances e.g. failure of credit decisioning system.
- Conduct regular scenario testing to validate continuity plans and tolerance levels.
- Uplift Business Continuity Plans using a critical operations lens to incorporate key changes.
- Monitor and report non-compliance with tolerance levels.
- Business led periodic testing (at least annually) to ensure the 'severe but plausible' scenarios are current, and the BCP remains effective.

Service Provider Management

- Identify and record all material service providers e.g. electronic lodgement and loan processing service providers, including any fourth/nth parties e.g. sub contractors to a mortgage broker. Submit register annually to APRA.
- Conduct due diligence before entering into new arrangements, or renewing or fundamentally changing existing arrangements.
- Contractual agreements with material service providers need to be uplifted to meet minimum CPS 230 requirements.
- Identify the key financial and non-financial risks for each material service provider. Map associated obligations, risks and controls.
- Monitor the effectiveness of the controls to manage the associated risks, remediate and report any resilience weaknesses identified.

Governance and Oversight

- Establish clear Governance and Accountability, including defined roles and responsibilities. The Board is primarily responsible for operational risk management and must oversee senior management's implementation and maintenance of CPS 230.
- Uplift Risk Management Framework including supporting policies and standards to include key changes.

How can we help?

Set up the right foundation

- CPS 230 readiness review, maturity and benchmarking assessment.
- Operational resilience Target Operating Model (TOM) design.
- Operational resilience program planning, scoping and delivery.

Increase Board and senior management accountability

- Operational resilience governance and accountabilities definition.
- Board and executive awareness sessions.

Identify critical operations

- Critical operations definition and documentation, including resources.
- Internal controls mapping, across the identified risks and obligations.

New operational risk management requirements

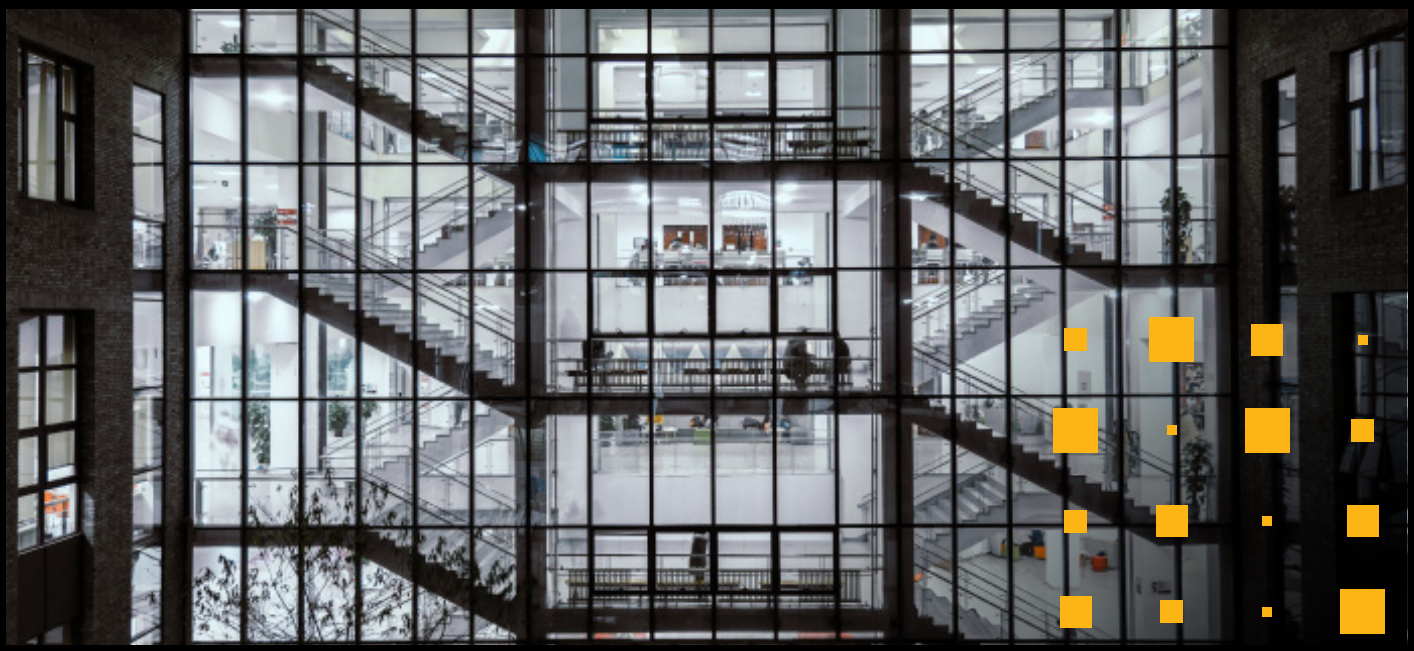
- Operational risk profiling (incl. risk appetite definition).
- Operational resilience review to identify potential resilience gaps in the environment.
- Controls assurance (incl. gap identification and remediation).

Set impact tolerances and perform scenario testing

- Impact tolerance identification.
- Business Continuity and Disaster Recovery Planning.
- Training and awareness.
- Scenario testing.

Determine Material Service Providers (MSPs)

- 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
T: +61 413 745 343
E: peter.malan@au.pwc.com

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

Sara Afaghi
Partner
Tel: +61 433 760 969
E: sara.afaghi@au.pwc.com

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

PWC200918366