Prudential Standard CPS 230

Operational Risk Management

APRA's release for consultation

Overview

What is APRA CPS 230?

On 28 July, APRA released a new cross-industry Prudential Standard CPS 230 Operational Risk Management (CPS 230) for consultation. This standard is designed to set out key requirements for managing operational risk, including updated requirements for business continuity and service provider management.

The objective of this standard is to strengthen the management of operational risk in the banking, insurance and superannuation industries and minimise the impact of disruptions to customers and the financial system.

The proposed CPS 230 will replace five existing standards: Prudential Standard CPS 231 Outsourcing, Prudential Standard CPS 232 Business Continuity Management and the equivalent superannuation and health insurance standards (SPS and HPS).

What will it cover?

There are 3 strategic focus areas in this proposed standard:

1. **Operational Risk Management:**

   Business-line management is required to take responsibility for the oversight and management of operational risk. It is expected that the **Board is accountable** for the oversight of operational risk management, and that senior managers within the business are responsible for the ownership and management of operational risk across critical operations.

   To strengthen **operational risk management**, APRA-regulated entities are required to conduct operational risk assessments to better understand and maintain their operational risk profile. This includes new products or changes that may materially impact the organisation's operational risk profile. In order to effectively manage key operational risks, entities must also design, implement and embed **internal controls**, along with processes to periodically **test and remediate** any identified weaknesses. **Operational risk incidents** and near misses are also to be identified, reported and addressed in a timely manner.

2. **Business Continuity Management:**

   In order to respond to increased digitisation within the industry, there is a need to evolve business continuity planning to focus on maintaining all critical operations for an entities' customers. It is important that all APRA-regulated entities are able to respond to disruptions and maintain critical operations such as payments, deposit-taking and management and customer enquiries. All APRA-regulated entities should identify their **critical operations** and deliver it within set **tolerance levels** for the maximum level of disruption they are willing to accept, with a credible **business continuity plan (BCP)** in place that is regularly **tested and reviewed.**

3. **Service Provider Management:**

   Requirements have been enhanced to cover **all material service providers** that APRA-regulated entities rely upon for critical operations or that expose them to material operational risk. Entities are required to understand and manage the risks associated with the use of service providers, along with their downstream providers (i.e. fourth parties), with a comprehensive outsourcing management **policy, formal agreements and robust monitoring**.

APRA's key timeline for the proposed standard

July 2022
Consultation open

October 2022
Consultation closed

Early 2023
CPS 230 finalised

January 2024
Effective date

APRA's timeline allows for one year between the final standard and full compliance. The breadth of change covered in CPS 230 will impact stakeholders internally and externally, including policy and contractual changes, as well as considerations on operating models and enabling tools to support the testing requirements. We recommend regulated entities begin planning now, with a view to stand up a program before the end of 2022 to support full compliance by Jan 2024.

pwc

Considerations for action

Move now, get ahead

Have you considered what the implementation of CPS 230 may mean for your organisation? How ready are you to comply?

Identify the additional requirements for operational risk, business continuity and material service providers. Identify the capability uplift required to meet requirements.

Who is a material service provider to your organisation? Do you have visibility over your downstream service providers? How have you managed the risks associated with outsourcing your critical operations?

Map and manage third and fourth parties at all stages of the arrangement. Review and renegotiate existing contracts if required. Outsource the service, don't outsource the risk.

Know your material service providers

Protect what matters

Have you identified key risks and controls supporting your critical operations? Are control gaps identified with remediation programs in place?

Perform regular risk assessments to understand the extended and changing landscape, develop and test controls, and monitor for operational risk incidents.

Does your board have oversight and senior management actively managing the resilience of your critical operations? How will you engage and set expectations with your key stakeholders?

Establish clear lines of accountability and oversight of your organisation's business continuity and the management of service provider arrangements to reflect effective risk management and decision making.

Accountable senior stakeholders

Response ready

Have you defined your critical operations? Are tolerance levels understood? Is testing and review conducted regularly?

Assess how a disruption may impact end users of your critical operations. Maintain updated business continuity plans that are well articulated and understood by the organisation.

How are you building resilience into your critical operations? How are you monitoring risk and resilience in your environment?

Identify clear metrics, measures and key controls which enable effective monitoring of operational risks. Where tactical measures are in place, create a roadmap to embed sustainable resilient practices.

Embed and monitor

Contacts

Please reach out to any of the below contacts should you wish to obtain further information.

Peter Malan

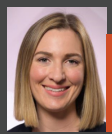
Partner | Cybersecurity & Digital Trust

P: +61 413 745 343
E: peter.malan@pwc.com

Nicola Costello

Partner | Risk & Controls Assurance

P: +61 467 607 785
E: nicola.costello@pwc.com



Noel Williams

Partner | Risk & Controls Assurance

P: +61 416 661 332
E: noel.williams@pwc.com

Bernadette D'Alessandro

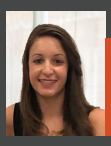
Partner | Risk & Regulation

P: +61 414 716 126
E: bernadette.b.dalessandro@pwc.com

Susanna Chan

Director | Cybersecurity & Digital Trust

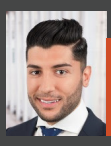
P: +61 414 544 066
E: susanna.chan@pwc.com



Joanna Del Vecchio

Director | Risk & Controls Assurance

T: +61 423 616 833
E: joanna.del.vecchio@pwc.com



Daniel Harb

Director | Banking & Capital Markets

P: +61 433 099 889
E: daniel.harb@pwc.com

Chris Davis

Director | Cybersecurity & Digital Trust

P: +61 400 388 087
E: chris.davis@pwc.com

Bevan Lim

Director | Risk & Controls Assurance

T: +61 411 405 980
E: bevan.lim@pwc.com

Natasha Kan

Senior Manager | Cyber-security & Digital Trust

P: +61 466 050 051
E: natasha.kan@pwc.com