KPMG

CPS 230 Operational Risk Management

APRA consults on a new prudential standard to strengthen operational risk management and operational resilience practices

The Australian Prudential Regulation Authority (APRA) has released a draft cross-industry Prudential Standard CPS 230 Operational Risk Management which has been designed to strengthen the management of operational risk by all APRA-regulated entities. The proposed standard underpins CPS 220 Risk Management and replaces several existing standards including CPS / SPS 232 Business Continuity management and CPS/SPS 231 Outsourcing.

It sets out revised operational risk controls and monitoring, business continuity and the management of service providers expectations. The key elements highlight a continued focus on operational resilience across the Australian Financial Services Sector.

Key elements of the draft CPS 230 are as follows:

Operational Risk Management

The need for a clear three lines of accountability for risk management:

1. The Board is ultimately accountable for oversight.
2. Senior management are responsible for the ownership and management of risk across end-to-end processes.
3. Business lines are responsible for the management of operational risk.

In addition, APRA is expecting that entities have:

- Clear processes and procedures to assess the impacts of new products, services, geographies and technologies on its operational risk profile, with commensurate changes in internal controls.
- Internal controls defined to detect and manage operational risks within appetite and meet compliance requirements.
- Incident management procedures to report and address any risk incidents and near misses in a timely manner.

Business Continuity Planning (BCP)

- BCP plans must reflect the current disruption landscape and continue to be appropriate to the nature, complexity and size of the entity.
- Cleary identify critical operations. While APRA has defined a number of these (e.g. payments, customer enquires), each entity will need to be specific on what it considers a critical operation.
- Define and establish Board approved tolerance thresholds and acceptable levels of disruption. This has seen a clear shift in the need to use the customer lens when assessing acceptable levels of disruption.
- Have a clear testing regime for its BCP which includes a range of severe but plausible scenarios to assess the ability of the BCP to meet the defined tolerance thresholds.

Service Provider Management

- Requirements have been extended to cover all material service providers.
- Define a comprehensive policy which covers how the entity will approach entering into, monitoring and exiting arrangements, and manage the risks associated with the use of a service provider.
- Identify material service providers, a provider which the entity relies on to undertake a critical operation or could expose the entity to a material operational risk.
- With the increase in complexity of supply chains, entities will need to define an approach to the identification of fourth parties in their supply chain and the management of these risks.
- Submit a register of material providers to APRA each year.
- Notify APRA of any new agreements with material providers which support critical operations.
- Notify APRA of any agreements, including changes to agreements where data or personnel are located offshore.

Consultation timeline

1 July 2022
Consultation Open

21 October 2022
Consultation Closes

Early 2023
CPS 230 Finalised

1 January 2024
Effective Date

Key considerations

In consideration of the proposed timeframe for implementation, we suggest APRA-regulated entities should start considering the key components of the proposed standard now, to ensure they are appropriately prepared. While the construct of the draft prudential standard may change, the key themes continue to be features of APRA's updated Corporate Plan, indicating they will remain areas of regulatory focus regardless of the outcome of the consultation.

Be prepared for risk events

Entities must ensure an effective process to support the management and response to risk events, effectively reducing their impact.

Be resilient

Entities must continue to operate through the ever increasing breadth of disruption, providing critical services to their customers.

Protect the entity & Community

Business continuity planning and exercising will be critical to ensure that the impact of disruptions is minimised to an acceptable/ tolerable level.

Operating Model	– How clearly defined and mature are your 3 Lines of Defence? – How well defined are your governance and reporting requirements? – Are accountabilities clear and understood?
Critical Operations	– Are your critical operations well defined? – Are all the supporting functions, processes and dependencies understood? – How do you set and measure tolerance thresholds and triggers?
Material Service Providers	– What does a material service provider mean to your entity? – How clear are you on the material service providers in your supply chain?
Business Continuity	– Is your Business Continuity Program fit for purpose, up-to-date and reflecting contemporary practices? – How do you approach the exercising and monitoring of business continuity?
Incident Management	– How mature is your approach to the identification and reporting of incidents and near misses?
Controls environment	– How do you establish an overall control framework including the design, monitoring and reporting of adequacy and effectiveness of key controls supporting operational risk and resilience?

As regulations and frameworks evolve, KPMG supports our global financial services clients across Europe, the UK and ASPAC to implement operational risk management standards. Through this work, we have developed deep experience and insight and are committed to supporting you to strengthen your operational risk and resilience practices.

Stay connected as we continue to provide thoughts, insights and share our learnings into this important regulatory change. Speak with us today for an individual briefing on what this will mean for you.

Contact us

Mark Tims
Partner
Technology Risk & Cyber
T: +61 2 9335 7619
E: mtims@kpmg.com.au

Gavin Rosettenstein
Partner
Operational & Third Party Risk
T: +61 2 9335 8066
E: gavin1@kpmg.com.au

Marie Chambers
Partner
Sourcing & Procurement Advisory
T: +61 2 9335 7124
E:mechambers@kpmg.com.au

Kat Conner
Partner
Risk & Regulation
T: +61 39346 563
E: katconner@kpmg.com.au

Campbell Logie-Smith
Director
Cyber Resilience
T: +61 3 9288 5920
E: clogiesmith@kpmg.com.au

KPMG.com.au

December, 2022. 1001924292MC.