

CPS 230 Operational Risk Management

Considerations for a periodic assurance review

APRA has released a draft cross-industry Prudential Standard CPS 230 Operational Risk Management 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 the requirement for a periodic assurance review of the Operational Risk focus areas, Business Continuity Plan and the management of service providers' expectations. The key elements highlight a continued focus on operational resilience across the Australian Financial Services Sector.

Operational Risk Management

- For the CPS 230 requirements specifically, ascertain whether an entity understand its risk profile, notifies APRA of security or material incidents within 72 hours and embeds internal controls in its products, processes and systems.
- Consider the assurance alignment and timing in conjunction with the:
 - CPS / SPS 220 Risk Management operating model review (encompassing Board accountability, reporting lines and clearly defined business line roles and responsibilities).
 - SPS 114 ORFR Assurance review for RSE licensees to determine if sufficient operational risk capital is being held.

Business Continuity Plan (BCP)

- Deliberate suitable approaches for assurance coverage based on the entity's maturity. This may incorporate a review of BCP Policies and Disaster Recovery Plans (DRP) clearly articulating each entity's ability to maintain its critical operations within measurable tolerances, through to a deep dive of critical supporting functions (e.g. Payments).
- Refresh the review procedures previously carried out to determine whether scenario simulation exercises and recovery testing activities are fit-for-purpose and adequately performed over critical operations (rather than on critical systems).

Material Service Providers (MSP)

- Obtain initial and ongoing assurance coverage of proposed and existing MSPs for critical operations (or MSPs that expose the entity to a material operational risk), with consideration to the comprehensive risk assessment required before providing services, and the results of CPS 234 reviews.
- Evaluate outsourcing, service management and procurement policies and procedures covering:
 - Definition and identification of the entity's critical operations and material operational risks.
 - How an entity approaches entering into, monitoring existing arrangements, and managing risks with a service provider's critical operations.
- Regular reporting to the Board on the entity's ability to comply with entity's service provider management policy for such arrangements.

Further considerations

Impact on coverage

- Consider how standardisation of assurance coverage across regulated entities can be more easily benchmarked across industry peers and global entity insights can be leveraged from UK's operational resilience standard.
- New prudential standard replaces 5 standards, and makes reference to 11 existing standards (with corresponding practice guides where relevant). How will this impact the alignment, scope and timing of the reviews when planning assurance coverage?
- Are subject matter experts available and capable to facilitate review (with relevant experience across operational resilience, service provider management and risk)?

Key concepts introduced

- Is the definition of critical processes and material weakness clear?
- Focus of new standard will be to review critical operations rather than critical systems. How will testing procedures be modified to incorporate this?
- How does the organisation define and measure tolerance thresholds and triggers?
- Would the scope of assurance review consider fourth party providers?
- How would APRA invoke the request for an independent operational risk review?

Controls environment

- How are all the supporting functions, processes and dependencies of your critical operations understood by your organisation?
- Are recommendation gaps proportionate to the urgency and level of prioritisation required based on size and complexity?
- How has the organisation established an overall control framework including the design, monitoring and reporting of adequacy and effectiveness of key controls supporting operational risk and resilience?
- To avoid the assurance review being a 'tick the box exercise' consider the quality and maturity of changes implemented to ensure it is fit for purpose.

Contact us



Ian Tracey
Partner
Internal Audit
T: +61 3 9288 5572
E: itracey@kpmg.com.au



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



Andrew Maudsley
Partner
Internal Audit
T: +61 2 9335 7267
E: amaudsley@kpmg.com.au



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



Suzanna Antoniou
Director
Internal Audit
T: +61 3 9288 6640
E: santoniou1@kpmg.com.au



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



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



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

KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2022 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

December, 2022. 1001924292MC.