CPS 230 Operational Risk Management

Alignment to existing regulatory architecture

Shortly after the Australian Prudential Regulation Authority (APRA) released a draft cross-industry Prudential Standard CPS 230 Operational Risk Management, it also released an information paper titled 'Modernising the prudential architecture'.

The information paper outlines plans for APRA to modernise the architecture of prudential standards and guidance for banks, insurers and superannuation funds which is a part of a multi-year program that commenced in 2021.

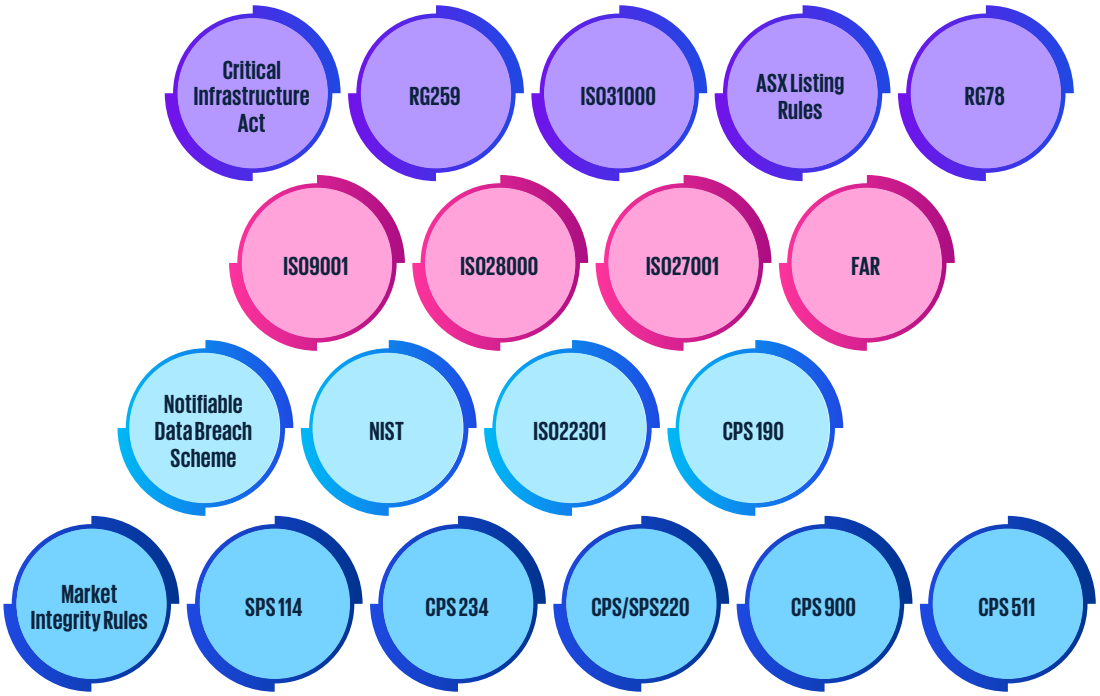
Draft CPS 230 is the first standard released under the direction of this program. The draft combines five existing standards (CPS 231 Outsourcing and CPS 232 Business Continuity Management and the corresponding superannuation standards SPS 231 and SPS 232 and private health insurance standard HPS 231).

In addition to combining these standards, draft CPS 230 intersects with a number of existing standards from both APRA and other regulators. If the standard is implemented in its current form, it will be important for entities to examine and consider these intersections in order to meet other obligations.

It is also important for non-regulated entities, who are engaged as suppliers for regulated entities, to consider how the draft CPS 230 requirements align to the standards and requirements which they currently meet.

Below are some of the requirements and industry standards which should be considered in conjunction with draft CPS 230. Refer to the following page for more detail on key requirements:

Draft CPS 230



CPS 220 / SPS 220 Risk Management	CPS 230 supports CPS 220 in the requirement for entities to develop and maintain a risk management framework. In terms of the reviews required under CPS 220, CPS 230 requires that these reviews must cover aspects of operational risk management and that operational risk management is integrated within the overall risk management framework and processes.
CPS 234 Information Security	Draft CPS 230 intersects with CPS 234 in terms of notification requirements. The reporting timeframes are the same (72hrs) and it is not intended that an incident reported under CPS 234 would need to be separately reported for CPS 230. However, there are overlaps with the requirements of notifications to other regulators such as the OAIC, ASX, AFP and ASIC which will need to be considered.
CPS 900 Resolution Planning & CPS 190 Financial Contingency Planning	CPS 900 links closely to the CPS 230 requirements related to the identification of critical processes. The CPS 900 critical functions are distinct to the critical operations as outlined in CPS 230 which focuses more on the processes to ensure it survives a disruption. However, there are elements of overlap around resolvability and pre-positioning activities and ideally both would be looked at concurrently. Broader linkage around CPS 190 (Financial Contingency Planning) and the various ICAAP/ILAAP, contingent funding and solvent wind down activities should also be considered and aligned.
SPS114 Operational Risk Financial Requirement	At this stage APRA does not propose to change the operational risk capital for ADIs and insurers and RSE licensees will remain bound SPS 114 in relation to the operational risk financial requirement. However, under draft CPS 230, APRA may require trustees to hold additional capital in the form of ORFR where their operational risk management has material weaknesses. APRA will provide further information at a later date.
ASIC Market Integrity Rules	New market integrity rules will apply from 10 March 2023 and are aimed at promoting the technological and operational resilience of securities and futures market operators and participants. There is a clear linkage between these requirements and CPS 230 in relation to business continuity and resilience requirements and notification obligations.
Modern Slavery Act 2018	The Modern Slavery Act requires that an Australian entity or an entity that carries on business in Australia with a minimum consolidated revenue of $100 million must submit a modern slavery statement for that financial year. A key part of this process is for entities to assess the risks of modern slavery in their operations and supply chains and for them to have a detailed understanding of their material service providers.
Critical Infrastructure Act	The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) came into effect on 2 April 2022. Following this, the Security of Critical Infrastructure Act 2018 was expanded to cover financial services organisations (including superannuation). The cross over with CPS 230 relates to incident reporting, the registration of critical infrastructure assets and the requirement to have a risk management program. There is also clear cross over with CPS 234.
Financial Accountability Regime (FAR)	CPS 230 describes the Board as being 'accountable' for the oversight of an entity's operational risk management and also outlines several responsibilities and accountabilities related to reporting. It will be important for entities to consider their approach to this in terms of 'reasonable steps' for those holding accountable positions under FAR.

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.