



# CPS230

## THE JOURNEY TOWARD RESILIENCE AND ADDING VALUE

### APRA'S NEW STANDARD ON OPERATIONAL RISK MANAGEMENT

By Jules Gribble,  
Jane Byrne, and  
Daniel Frank

APRA is putting a lens on operational risk management for all APRA regulated entities and will require greater focus on operational risks from the Board and management.

**PFS Consulting can help you  
navigate this journey**

#### Key points

- CPS230 consolidates, refines, and streamlines several current standards, as well as introducing some new requirements with a focus on improving resilience of entities in times of stress
- Compliance with the new standard should be thought of as a foundation on which to consolidate and build out risk maturity
- Properly considering the longer-term benefits, utilising the right methodologies and tools, and staying the course will deliver value

#### CONTACT



**JANE BYRNE**  
janebyrne@pfsconsulting.com.au  
Phone: (02) 9225 6100



**JULES GRIBBLE**  
julesgribble@pfsconsulting.com.au  
Phone: (02) 9225 6100



**DANIEL FRANK**  
danielfrank@pfsconsulting.com.au  
Phone: (02) 9225 6100

APRA has recently published its draft CPS230 'Operational Risk Management' for consultation. The purpose of CPS230 is given in its first line: '... to ensure that an APRA-regulated entity is resilient to operational risks and disruptions.' To encourage improving entity resilience, APRA is consolidating several current prudential standards into a single standard that covers all the industries it supervises (superannuation, life, general and health insurance, and banking).

CPS230 provides an opportunity for regulated entities. Complying with the APRA's minimum standards is clearly required, but the opportunity for entities is to step beyond seeing this as another regulatory burden and extract value from it.

Managing operational risk should also be an integral part of an entity's overall risk management frameworks, risk appetites, and processes. Compliance provides a foundation that enables building the house of risk culture. Organisations with strong and mature risk cultures are more efficient and effective in achieving their strategic aims, increasing value, and are more resilient under stress.

PFS Consulting can support regulated entities on their journey toward resilience and adding value by:

- Reviewing and consolidating their approaches to risk management, especially for Operational risk, and assess where they are relative to where they want to be, and
- Building on the compliance foundation to support improving their risk culture, risk maturity, and resilience.

We comment on why CPS230 is timely, what it covers, and the key role of compliance. To progress on the journey toward resilience and adding value, assessment tools and maps for next steps are needed. We support this by applying methodologies that provide transparent assessment and management tools.

### Why now?

Attitudes toward risk management, operational risk management in particular, can be seen as 'lighting rods' that provide insights into broader corporate and risk management attitudes and cultures.



Throughout the financial services industry there are many significant changes occurring:

- A quickening pace of technological change and its consequences'
- The need to address changing client needs and expectations; and
- Increased supervisory activity and expectations from both APRA and ASIC.

These underlying challenges are not restricted to specific events but can permeate entities and their cultures all the way to the top.

Within entities the pace of change and increasing complexity makes operational risk management an ongoing challenge. The risk of major, possibly entity ending, operational risk events occurring is ever present. The out-workings from the Hayne Royal Commission continue to ripple out, and examples of poor practices continue to mount. We are also seeing increased supervisory activity and expectations from both APRA and ASIC.

Every entity faces operational risks and needs to identify and mitigate the impact of future risk events and manage the risk events that occur. With the increasing pace of change, stresses, and complexity in financial services, it is clear that risk events will occur for all entities. The challenge is how these risks and risk events are detected, mitigated, and addressed.

It is perhaps no coincidence that APRA has released its draft of CPS230 now. Across all aspects of operational risk uncertainty and change are dominant features.

Focusing on operational risk and its management now seems unashamedly prudent.

## CONTACT



**JANE BYRNE**

janebyrne@pfsconsulting.com.au  
Phone: (02) 9225 6100



**JULES GRIBBLE**

julesgribble@pfsconsulting.com.au  
Phone: (02) 9225 6100



**DANIEL FRANK**

danielfrank@pfsconsulting.com.au  
Phone: (02) 9225 6100



### What is CPS230 about?

CPS230 seeks to 'lift the bar' around operational resilience and is an opportunity for entities to improve their value through improved risk management and strengthening risk culture, especially during periods of uncertainty. From the beginning of 2024 a finalised CPS230 is expected to apply to all financial services entities regulated by APRA. This broad applicability emphasises some key points:

- The universal nature of operational risk. All entities face operational risks whatever sector they operate in. Operational risks are amplified for financial services as these services are long-term, generally abstract in nature, and important to individuals.
- The need and benefit of taking a holistic view. Across entities and sectors, the products/services, objectives, and priorities may change but the need to manage these key risks do not.
- Prevention vs cure. There are essentially two perspectives on risk events. Initially, there is a focus on prospective mitigation of risk events. When risk events occur, there is then a focus on risk event management.

The importance that APRA places on operational risk management is apparent from the draft CPS230 and several recent speeches by senior APRA representatives, particularly when considering the broader concept of operational resilience. CPS230 also needs to be considered in the context of related APRA requirements, such as CPS/SPS220 (Risk management). The importance of operational risk management for APRA regulated entities is also shown by its profile in APRA's Supervisor risk and intensity model.

### CPS230

- Introduces some new ideas but is also a synthesis, consolidation, clarification, and refinement of current requirements. It now includes traditional operational risk topics, business continuity, and outsourcing requirements.
- Reflects the breadth of operational risk as it now specifically includes legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk, and change management risk as part of operational risk. This now covers both financial and non-financial risks.
- Broadens the scope of operational risk management and enhances its standing in an entity's risk management framework. Importantly, CPS230 emphasises the importance of the Board's role in establishing effective risk management frameworks by determining policy, setting risk appetites, and establishing appropriate processes for monitoring, analysis, reporting and managing risks and risk events.

### Role of compliance

From a supervisory perspective, there is naturally a strong focus in CPS230 on compliance. We suggest an initial focus on addressing compliance requirements efficiently may be appropriate, although the longer-term goal of value creation should be kept in mind. Meeting compliance requirements is a necessary minimum level for acceptable business practice. While compliance is a critical step, it is a means to an end, but is not the end in of itself. When compliance is done right, it can form the foundation for improved risk maturity and increased value.

Having said that, we understand that addressing compliance requirements is often a significant task, and so it is important to have ways to manage that process. This leads to methodologies that identify where an entity is on a risk maturity scale, identify areas for improvement, and assess the impact of changes from a cost-benefit perspective, both from an immediate financial perspective, and potentially more broadly.

We also believe that the task of meeting CSP230 requirements provides entities an opportunity to consolidate existing compliance arrangements, operational risk processes, and good practices. These may have developed over time in different strands and in different parts of the organisation. CPS230 can be a catalyst to integrate these elements into a cohesive whole.

### CONTACT



**JANE BYRNE**

janebyrne@pfsconsulting.com.au  
Phone: (02) 9225 6100



**JULES GRIBBLE**

julesgribble@pfsconsulting.com.au  
Phone: (02) 9225 6100



**DANIEL FRANK**

danielfrank@pfsconsulting.com.au  
Phone: (02) 9225 6100

## The journey

The first step is to identify an entity's current place in its risk maturity journey. We start by identifying the gaps in compliance and then proposing actions required to meet them which identifies where an entity is with its risk compliance requirements.

An entity's Risk register and Risk Event register provide assessments of the impacts of risks the entity has identified it faces. PFS can apply its methodology for assessing a risk register to provide an assessment of the overall impact of the risks included in an entity's Risk Register. In parallel, an entity's risk culture needs to support its approach to risk.

For boards to effectively implement a robust risk management framework, both the appropriate risk management processes (including compliance) and risk culture need to be in place.

We can provide a path forward which includes discussions about operational risk management objectives and developing a roadmap to achieve them. In this way, an entity can benefit by considering how they address operational risk management in the longer-term and avoid a short term, but natural, tendency to focus on addressing short term issues by just complying with new requirements.

The outcomes from this process will vary depending on the entity's level of risk maturity. The methodology can be tailored to a particular entity's needs and then applied as a management tool for moving forward as expected consequences of actions can be assessed and then reported against.

## Conclusions

The risk management frameworks entities have in place, including comprehensive internal controls, lay the groundwork for improving risk maturity. Improving risk maturity is key to improving resilience and adding value for stakeholders. The effectiveness of risk management (policies, processes, and culture), how this is embedded within an entity, and how it operates, is core to its long-term effective operation.

### CPS230

- Provides an opportunity for entities to use compliance as a lever to improve risk maturity and business practices for the benefit of both businesses and their customers, policyholders, or members
- Puts a lens on operational risk for all APRA regulated entities and will require greater focus on operational risks from the Board and management. This is an opportunity for entities to improve their operational resilience and add value to their stakeholders
- Introduces some new operational risk management requirements building on, consolidating, and refining current requirements
- Supports compliance as an initial step in the journey toward improving an entity's resilience and risk maturity, increasing stakeholder value

**PFS can support entities realising and increasing value by applying the appropriate tools and methodologies that:**

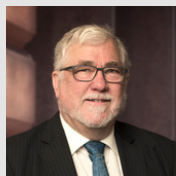
**Help entities review their current status,  
Identify gaps between this and their desired status, and  
Provide a management tool to support making that transition.**

## OUR TEAM

We would be pleased to discuss your operational risk management journey with you. Please contact:



**Jane Byrne**  
Director



**Jules Gribble**  
Principal



**Daniel Frank**  
Senior Consultant