PFS CONSULTING

FORESIGHT INSIGHT OVERSIGHT

OPERATIONAL RESILIENCE: A BIGGER GAME AND A BROADER PERSPECTIVE. HOW WILL YOU EXPLOIT THIS OPPORTUNITY?

By Jules Gribble
PFS Consulting, Principal

KEY TAKEAWAYS

- **The key new aspect of CPS230 is its holistic focus on operational resilience, with a 'success test' of maintaining consumer service adequacy under the stress of disruption events**
- **All businesses face operational risks and disruption events will occur. The challenge is how to effectively address these disruption events**
- **The opportunity offered in the implementation of CPS230 is the consolidating and coordinating of operational risk polices, processes and practices, improving risk maturity and adding value**
- **The explicit focus of operational resilience on consumer outcomes is new and is a 'game changer' as it moves assessment of an entity's success from internal to external, with consumers being the judge**
- **APRA's current focus on operational resilience will become a permanent aspect of prudential supervision**

CONTEXT

In July 2023 APRA published its new Operational Risk Management Prudential Standard, CPS230, which comes into force on 1 July 2025. To date there is no accompanying explanatory CPG230.

PFS Consulting discussed a draft CPS230 in September 2022 and provided further commentary after the final CPS230 was published in July 2023.

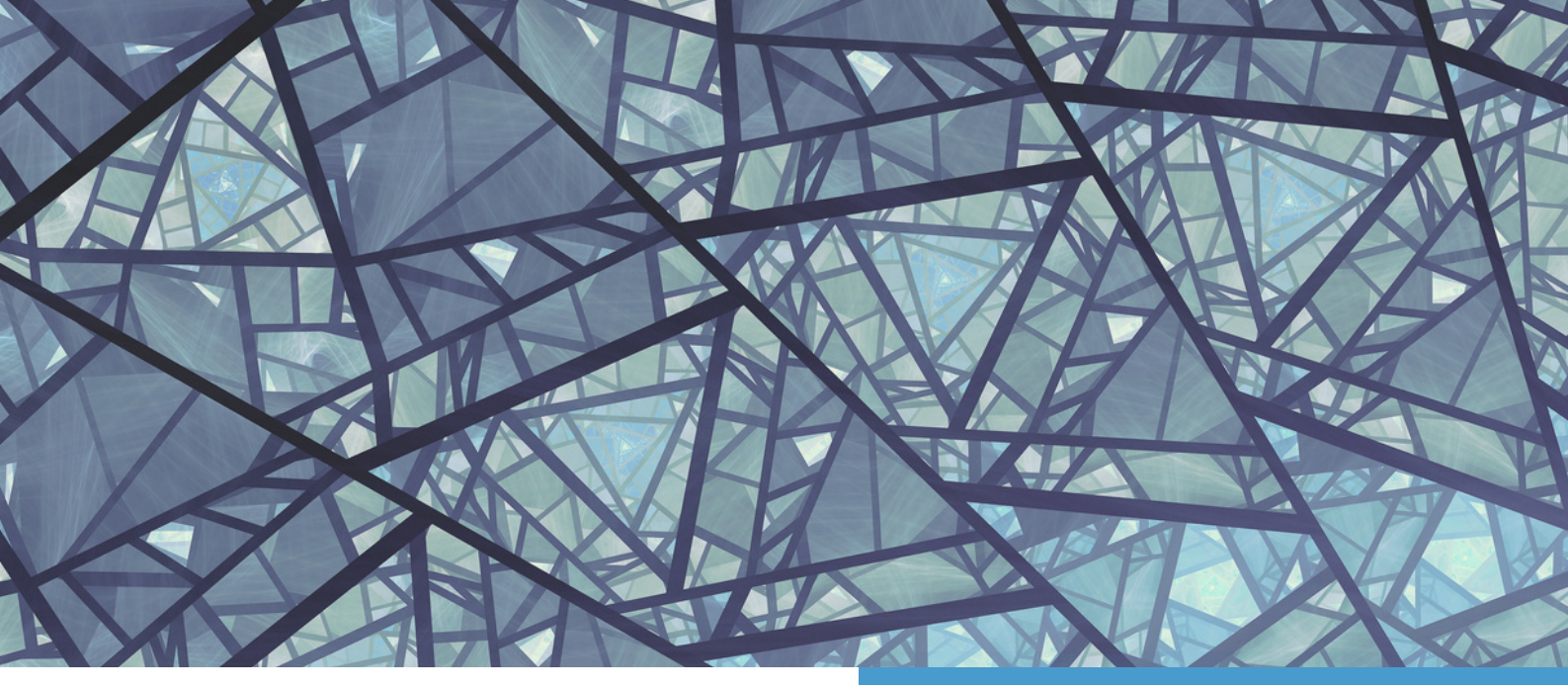
CPS230 applies to banks, insurers, and superannuation funds, so its relevance is universal across financial services. While the importance of specific risks may vary between entities, all face operational risks and operational risk events simply by virtue of being in business.

PFS continues to emphasise the opportunity for organisations to gain a sustainable value premium from effectively implementing CPS230 and recognising the importance of improving and deepening their risk culture.

CONTACT

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

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



APRA has stated operational resilience is one of its four key priorities in its 2023-24 Corporate plan: 'a heightened focus on operational resilience, including cyber resilience, crisis management and operational risk management, to maintain the continuity of critical financial services'.

This emphasises the importance of CPS230 and there are continuing references to the CPS230 framework for managing operational resilience when more detailed guidance is being provided on specific aspects of that framework. See, for example, APRA's November 2023 Insight article.

This article steps back from the specifics of CPS230 to review its origin and give our take on its underlying intentions.

OPERATIONAL RESILIENCE

APRA uses the phrase 'operational resilience' twice in CPS230 but unfortunately, the term is not explicitly defined.

We define operational resilience as:

The capacity of a (financial services) entity to:

- Prevent disruption to the critical services they provide to consumers the extent practicable,
- Adapt systems and processes to continue to provide critical services and functions when a disruption event occurs,
- Return to normal running when the disruption event is resolved, and
- Learn and evolve from both disruption events and near misses.

A BIGGER GAME HAS STARTED

Achieving operational resilience may require review and update of policies and processes to improve their resilience and robustness in unexpected and stressed situations, 'Business Not as Usual' (BNaU), in contrast to 'Business as Usual' (BaU) and expected situations. Actions appropriate in a familiar BaU context may be inappropriate in an unfamiliar and possibly rapidly evolving BNaU context. The concept of operational resilience highlights a realignment of perspective to focus on consumer outcomes with the objective of minimising the impact of disruptions on services provided to consumers. That is, the 'success test' of effective operational resilience is the extent to which critical consumer services are maintained in a disruption event.

Jules Gribble
PFS Principal

Business efficiency and effectiveness may now need to be assessed in light of adequacy of capacity in both BNaU and BaU circumstances. For example, this may require the introduction of some redundancy to avoid single point dependencies to improve robustness in BNaU situations.

Do you remember the adverse impacts 'just in time delivery' had during the recent COVID pandemic? It may also be salutary to think of the sinking of the 'unsinkable' Titanic in 1912. In its original design, the hull was divided into compartments intended to contain water if a leak occurred. As a cost efficiency (cutting) measure, the walls of these compartments were not extended up to the deck, leaving gaps at the top which water could pass through. The Titanic encountered a (very) BNaU situation by hitting an iceberg, filled with water, and sank with great loss of life.

The importance of managing BNaU situations is relevant to all entities and is emphasised by the rise of major cyber security incidents, failures of third parties, and increasing risks of sophisticated technology. We are all aware of major issues arising in Australia in recent times that indicate serious operational risk events, questions about management responses, and deficiencies in supporting processes. Significant reputational harm can, and has, also be incurred.

GLOBAL PERSPECTIVE

The Bank of International Settlements (BIS) published 'Principles for Operational Resilience' in May 2021. This document outlines principles of operational resilience in the banking context. Supervisors globally, including APRA, have recognised these principles are applicable in all financial services domains, including banks, insurance, and superannuation.

These principles are being implemented globally by supervisors, including the PRA in the UK, the DORA legislation in the EU, supervisory publications in the US, OSFI in Canada, the Hong Kong Monetary Authority and, of course, APRA in Australia.

The BIS principles, slightly amended to reflect their more universal relevance, are:

Principle 1: Governance and leadership. Financial services entities should utilise their existing governance structure to establish, oversee, and implement an effective operational resilience approach that enables them to respond and adapt to, recover from, and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.

Principle 2: Operational risk management. Financial service entities should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes, and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience approach.

Principle 3: Business continuity.
Financial services entities should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.

Principle 4: Interconnection and interdependence of critical operations.
Once a financial services entity has identified its critical operations, the entity should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

Principle 5: Third-party dependency.
Financial services entities should manage their dependencies on relationships, including those of, but not limited to, third parties or intragroup entities, for the delivery of critical operations.

Principle 6: Incident management.
Financial services entities should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the entity's risk appetite and tolerance for disruption. Entities should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

Principle 7: Resilient technology and decision making to facilitate delivery of critical operations.
Financial services entities should ensure resilient information and communication technology including cyber security that is subject to protection, detection, response, and recovery programmes that are regularly tested, incorporate appropriate situational awareness, and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.

These principles provide the basis and a framework for many fundamental discussions, some of which are introduced below.

A summary might be:
operational resilience is underpinned by operational risk management and its component subject areas including operational risk event management, business and business continuity management, disaster recovery, crisis management, change management, technology and cyber risk management, third-party risk management, and data risk management. That is, all the areas that can be included under the traditional definition of operational risk: the failure of people, processes, or systems, including external events, reputational and legal risks, and now increasingly business and strategic risks, with the 'success test' described above attached. This is an extensive canvas to paint operational resilience on.

Experience overseas has highlighted that implementing operational resilience may be a large, time consuming, and ongoing task. There is no reason to believe the Australian experience will be any different, although we may gain some benefits from examining that overseas experience.

A NEW PARADIGM

The crucial learning to take from the above principles is that the focus is now on consumer outcomes. That is, the effective 'success test' of operational resilience lies with the success and robustness of an entity's continuation of processes and services in the face of disruption. This test is in terms of consumer/user outcomes, not in terms of internal entity process or perspectives. It is about maintaining critical services to consumers under duress.

The explicit focus on consumer outcomes is new and is a 'game changer' as it moves the assessment of an entity's success from internal to external, with consumers being the judge.

PROCESS FOR MANAGING OPERATIONAL RESILIENCE

A standardised approach to addressing operational resilience is emerging, with the key steps being for entities to:

1. Govern and implement their strategy and approach to operational resilience, operational risk, and operational risk events with a management framework including reported through the appropriate processes and structures.
2. Identify its critical operations and map internal and external dependencies.
3. Establish tolerances for the disruption of critical operations.
4. Develop and regularly conduct scenario testing on critical operations to gauge its ability operational ability to operate within established tolerances for disruption across a range of severe but plausible operational risk events.
5. Establish an enterprise-wide operational risk management framework as part of its broader ERM strategy and framework.
6. Set risk appetites for operational risk and operational risk event management,
7. Ensure comprehensive identification and assessment of operational risks and operational risk events applying appropriate operational risk management practices.
8. Conduct ongoing monitoring of operational risk to identify control weakness potential breaches of limits/thresholds, provide timely reporting, and escalate significant issues.
9. Assess the effectiveness of their operational resilience policies and practices by applying the 'success test' of maintenance of critical services to consumers during disruptive events.

These implementation steps are reflected in CPS230 (except step 9). We observe that ASIC has also become involved with operational resilience for the superannuation industry with its new 2024 priorities, including a new priority around member services failures reflecting an end user focus.

We emphasise the practical reality of managing operational resilience is not about formal compliance reporting systems, which are a necessary but not sufficient step for success, but it is about the risk culture and risk maturity of each organisation and its understanding of the opportunities driven by CPS230 requirements that can be siezed upon to benefit the organisation.

That is, the key is how the data reported by compliance systems is used and analysed by management, rather than the reporting in of itself.

PFS CAN SUPPORT YOUR CPS230 JOURNEY

Implementing CPS230 provides an opportunity for entities to realise a sustained increase in value, improve the robustness of their processes, and improve their reputation and consumer satisfaction.

How are you planning to exploit the opportunity of CPS230 framework and extract these benefits for your organisation?

We can support you achieve your objectives by:

- Helping you review your current status,
- Helping you determine your desired status and identify gaps,
- Providing methodologies and management tools that support your governance and bridging those gaps, and
- Helping you develop your risk maturity to support entrenching your value gains.

We would be pleased to discuss your continuing operational resilience journey with you.

OUR OPERATIONAL RESILIENCE TEAM

Jules Gribble
Principal

Madeleine Mattera
Principal

Jane Byrne
Director

Daniel Frank
Senior Consultant

CONTACT

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

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