All Actuaries Summit
New age, new actuary

11-13 June 2025, Sydney

Actuarial Outreach:

Taming the Operational Resilience Hydra

Prepared by Jules Gribble

Presented to the Actuaries Institute

2025 All-Actuaries Summit

11-13 June 2025

Table of Contents

Abstract

On 1 July 2025, financial services enter a new age with the commencement of CPS 230:Operational Risk Management. The requirements of this prudential standard reflect a paradigm shift in how operational risk and related issues are to be managed. The core requirement of resilience reflects the need to maintain critical services through disruption. The success test of operational risk management is now the extent to which consumer expectations continue to be met under stress.

Risk management often implies the capacity for quantitative modelling. Uncertainty management reflects the broader need to address possible adverse events more qualitatively when they cannot be directly modelled but still need to be considered (NIL is a poor estimate). Operational risks, in the broad sense, represent a material portfolio of possible future adverse events that entities need to manage. Portfolios do not behave as their individual components do, so a process for aggregating risk impacts to generate a portfolio outcome is required. Having consistency between the risk profiles provided by Risk appetite statements and the aggregate profile generated by Risk registers seems a key requirement of operational risk and ERM more broadly.

Our approach, applied in an operational risk context, provides a tool that accommodates both qualitative and quantitative assessments and facilitates reconciliations between risk appetite and portfolio risk register profiles. We combine actuarial and other risk management expertise to deliver powerful tools that can provide management with clearer insight into their operational risk management by better understanding how their Risk appetite and Risk register profiles interact. The quantitative actuarial contribution to these processes is needed for them to work, but also requires the quantitative context and contributions that other professions can deliver. A combined interdisciplinary approach provides outcomes and insights that neither component can provide individually. Our approach applies actuarial expertise that when combined with the perspectives of other professions, leads to more balanced and robust insights and outcomes.

Keywords: Aggregation of risks, Business as Usual, Business Not as Usual, CPS230, CPG230, Critical operations, Critical services, Disruption, Governance, Culture, Operational risk, Operational resilience, Portfolio of risks, Qualitative risk management, Quantitative risk management, Risk culture, Risk management, Risk maturity

1 Context

1.1 Environment

On 1 July 2025, the Australian APRA regulated financial services all enter a new era with the commencement of Cross-Industry Prudential Standard 230: Operational Risk Management (CPS230), see CPS230. CPS230 is supported by CPG230, the accompanying Cross-industry Prudential Practice Guide, see CPG230. Note that CPS230 applies across all regulated financial service entities without distinction.

All Australian Systemically Financial Institutions (SFI's) are expected to fully comply with CPS230. On 30 June 2024, APRA's list of SFI's included 14 Approved Deposit Institutions, 4 General Insurers, 4 Life Insurers, and 24 Superannuation entities. Loosely, all the major players. Non SFI designated financial institutions have some time relief on some topics until 1 July 2026, when they are all then also expected to fully comply with CPS230.

The introduction of CPS230 is not occurring in isolation. A global trend was initiated by the Bank of International Settlements (BIS) in its 2021 document, Principles of Operational Resilience. See BIS 2021. Global take-up of the concept has been broad. See IIF 2024. In the EU, the Digital Operational Resilience Act (DORA) officially started in January 2023 with full compliance expected by January 2025. In the UK, the FCA set out final rules for Operational Resilience in March 2021 (PS21-3) with full compliance expected by the end of March 2025. In Canada, OSFI publishes its operational resilience requirements (Guideline E-21) in August 2024, with full compliance expected by September 2026. Experience shows that implementing operational resilience requirements can be time consuming, resource intensive, and have far reaching implications. Australia's timetable may lag some others, but we can gain the benefit of reviewing other experiences.

CPS230 uses the words 'operational risk' in its title, but it really discusses the broader concept of operational resilience. This is new and is a potential 'game changer' for all regulated financial services entities.

APRA uses the words 'operational resilience' twice in CPS230, but the term is not explicitly defined. CPG230 gives some insight in terms of outcomes:

> *Operational resilience is the outcome of prudent operational risk management: the ability to effectively manage and control operational risks; limit disruptions; and maintain critical operations through disruptions.*

The determination of what operations are critical, subject to APRA guidance, lies with entities. The determination of maintenance is effectively specified by APRA in CPS230 paragraph 35 and its 'material adverse impact' criterion:

> *Critical operations are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system.*

For clarity, we define operational resilience as:

Operational resilience is the capacity of a (financial services) entity to:

- *Apply appropriate operational risk management policies and procedures in standard business situations (that is, not under disrupted conditions)*
- *Prevent disruption to the critical services they provide to consumers to the extent practicable and within specified tolerances,*
- *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.*

This definition assumes that the disruption ends and a return to prior standard business situations occurs. If the disruption cannot be resolved or becomes permanent in some way, for example, a war, then the standard business situation has changed, and this should lead to more widespread reviews of policies and processes to address the 'new normal'.

This definition also assumes that the disruption is not so large that the entity cannot survive, that is, it is 'manageable'. Circumstances where the entity does not survive seem outside the scope of CPS230, although they may be addressed through resolution processes.

1.2 APRA expectations

APRA places a high priority on CPS230. This is shown by statements in various speeches and APRA's current 2024-25 Corporate plan about the importance of increasing the minimum standards for operational resilience through the implementation of CPS230 and the raising of industry standards on cyber risk management. Cyber risk is an operational risk, even if it has been singled out for special treatment.

Note the word 'minimum' in APRA's stated focus. In a regulatory environment where there is an 'at all times' expectation by supervisors, it is perhaps imprudent to only seek to meet only minimum requirements. Unavoidable and random business and environmental fluctuations will likely mean that at some time(s) minimum requirements will be breached. It is therefore prudent and expected by both supervisors and the wider community that minimum requirements are exceeded, perhaps significantly. To illustrate this, we observe that the capital ratios for both life insurers and general insurers, overall, are approximately 2. That is, these industries, on average, hold about twice as much capital as the minimum prescribed requirements.

We also note that APRA is moving past focusing primarily on financial resilience, without downgrading its ongoing importance, especially in turbulent times, and increasingly focusing on non-financial resilience in a coordinated manner. This process has been underway for some time and is entrenched in its published corporate plans. Operational resilience is an important component, but so also are a range of other reforms, including raising the standards of governance in regulated entities.

1.3 Our perspective

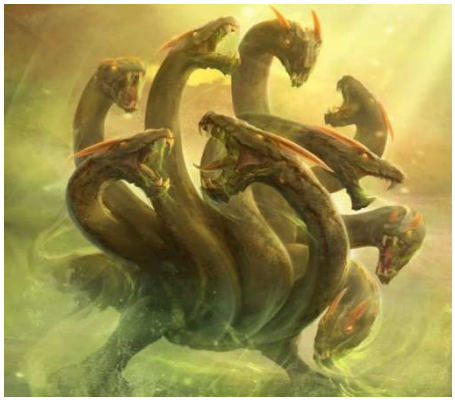
Many service providers are offering 'solutions' for CPS230 compliance. These offerings often include systems for monitoring compliance with CPS230 requirements and associated risk management. Note the word compliance. While there is clearly a need to demonstrate compliance with the minimum CPS230 requirements, we suggest this may miss the 'big game' and the benefits that may be accrued by understanding the bigger game better.

As noted above, meeting minimum prescribed requirements is unlikely to be a sufficient condition for success, although it is likely a necessary condition. For example, putting down the foundations for a building and including key components starts the process. As far as they go, the foundations may be fine, but they are not the building or how it is used or lived in. We have building codes and building inspectors to safeguard public interest. In the financial services industry, we have regulators and supervisors to safeguard the public interest. The level of protection is often higher in the financial services than more generally, as financial matters are critical to almost all aspects of our lives, livelihoods, and retirements.

To better understand the building we want to build and how it may be used, we step back from the specifics and examine the broader framework. Then we can come back to the specifics, CPS 230, in more detail, but with a clear view of the underlying objectives and how we may assess if they are being achieved.

1.4 Hydras[1]

Before going on, consider the classical Greek story of the hydra and its slaying by Heracles as the second of his twelve labours. The core immediate challenge of this was that each time a head of the hydra was cut off, two more grew in its place. The hydra was a monstrous nine headed serpent that lived in a swamp and raided nearby cattle farms for food.



Nobody was very happy.

Heracles employed lateral thinking to address his problem. After cutting off a head, he had his nephew immediately cauterise the stump to prevent regrowth. The points here are the lateral approach (not traditional or established, thinking), the capacity to implement it, and the need for teamwork. Heracles also gained some additional benefit from slaying the hydra, as he dipped his arrowheads in its poisonous blood and then could use these poisoned arrows for his future benefit.

More recently, the metaphor of the hydra has come to mean a difficult situation that is multi-dimensional, serious, may be evolving over time, and without clear

[1] An alternate meaning of 'hydra' is biological, a tiny, jellyfish-like creature that lives in freshwater. Hydra is also a beautiful 'get away' Greek island in the Saronic Gulf near Athens.

solution(s) or mitigations. There is a clear analogy with risk management. While we may believe we have identified and mitigated known (material) risks, new risks, or reinvigorated older risks, continue to emerge.

Reactive work is needed to address and manage known risks, although perhaps 'fighting the last war', and proactive work is needed to identify and prepare for new challenges, unknown risks, and 'fighting the next war'. These two tasks require different tools and attitudes and may apply very different approaches. They also require acceptance that the risks of human error and complacency always remain. There is also a clear distinction between addressing future risks, known or unknown, and managing risk events once they occur. In the hydra context, this is the difference between preparing a strategy to fight it and actually fighting it and dealing with the unexpected and immediate additional challenges of this.

We may not be able to slay the operational resilience hydra, but we can seek to understand it, mitigate its impacts, and limit adverse outcomes.

Our hydra metaphor focuses on the operational resilience context, but it applies equally in a broader Enterprise Risk Management (ERM) context.

2 Operational risk and operational resilience

We build on some work previously published. See PFS 2023a, PFS2023b, and PFS 2022.

2.1 Operational risk

The standard high-level definition of operational risk is typically

> *The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.*

A slightly more detailed description of loss event types is below, and lower-level taxonomies are also available:

Processes

- Execution, delivery, and process management
- Clients, products, and business practices

People

- Internal Fraud
- Employment practices and workplace safety

Systems

- Business disruption

External events

- External fraud (including cyber and technological)
- Damage to physical assets
- Other events (such as pandemics)

This specification is very broad and encompasses many factors that can disrupt business operations and lead to losses of some type, financial, reputational, or other. Operational risks are inherent in all business activities, including those of financial services entities.

The focus of the definition of operational risk is inward to the entity. It presumes that all appropriate governance strategies, policies, frameworks, and reporting are in place as part of the overall entity governance and ERM management. The effectiveness of operational risk management, the appropriate implementation of the required processes, people, and systems, underpins the effective management of all other risks the entity faces.

Paragraph 24 of CPS230 is noted here for some specific inclusions into the above general definition:

> *An APRA-regulated entity must manage its full range of operational risks, including but not limited to legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, and change management risk. Senior management are responsible for operational risk management across the end-to-end process for all business operations.*

While reputation risk is not explicitly included in APRA's list for CPS230, it is mentioned in CPG230. APRA addressed reputation risk outside CPS230. However, reputational risk is often now included under a broader operational risk umbrella, and it is difficult to see how it can be ignored when addressing operational risks and managing the provision of critical service to customers during disruptions or more generally. While its impacts can be hard to model, it can nonetheless be a potent force, so it needs to be considered.

The obligation to manage the full range of operational risks applies whether or not disruptions may occur.

A crucial aspect of effectively managing operational risks that is implicit, but not explicit, above, is the key role that culture, risk culture, and an organisation's leadership play. These things may be harder to measure and monitor, but they are nonetheless essential to long-term entity success.

2.2 Resilience

In general, resilience is understood to represent the capacity of individuals and entities to manage and recover from adverse situations or experiences.

From an organisational perspective, including financial service entities, resilience implies the capacity to continue operating and delivering services to customers (account holders, insureds, members, etc), within specified tolerance levels, both individual and corporate, through disruptions. The tolerance levels are expected to be set so that there would not be material adverse impacts on an entity's depositors, policyholders, beneficiaries or other customers or its role in the financial system. The level of disruption may also vary. For example, in terms of scale for a single entity, an industry, and/or geographical scope. In a globally connected world with very rapid electronic communication, the source of a disruption may be overseas, happen very quickly, and be out of the control of any local Australian authority.

2.3 Disruptions - Business Not as Usual

Material or significant disruptions, while hopefully not common, imply that the operating environment moves from 'Business as Usual' (BaU) to a 'Business Not as Usual' (BNaU). In a BNaU situation, it may be unreasonable to expect standard BaU processes to apply, so alternatives may be needed. Doing this under the stress of an unfolding situation can lead to poor and sub-optimal outcomes, so prior consideration in an unstressed context can be valuable. That is why Business Continuity Plans are developed in advance.

Every material risk event that occurs is, almost by definition, a BNaU situation. If it has been previously identified as possible, occurrence may be unexpected since mitigations are presumed to have reduced the frequency of occurrence to acceptable levels and also, hopefully, the severity of their expected impact. Such risks should be included in a Risk register and be expected to have had some modelling and analysis done to assess how they may be addressed. Other events will be unexpected, and so it is less likely that work has been done on how they may be addressed. These risks are unlikely to be included in the Risk register and so may need different, more ad hoc, and qualitative approaches initially used to address them. In these circumstances, scenario testing of more extreme but ill-defined (a priori) events can be valuable in developing practical and pragmatic resilience capacity under simulated BNaU conditions. The benefits of this should not be underestimated.

It is one thing to have a plan that has been developed, with good intent, in an unstressed context that meets minimum regulatory and other good practice requirements. It is a very different thing to be in a stressed situation as it unfolds and to seek to apply that plan.

We emphasise this with some famous quotes and a short story:

- *Plans are worthless, but planning is everything*, Dwight Eisenhower
- *No plan of operations extends with any certainty beyond the first contact with the enemy's main force. Only the layman believes that the course of a campaign follows a predetermined course which has been planned in detail in advance,* and *Strategy is a system of expedients.* Helmut von Moltke
- In the Twin Towers terrorist attack of 11 September 2001, a group of employees was saved because they had practiced the actual evacuation process (going down many flights of stairs) so that when the disaster occurred, they did not 'freeze', knew what to do, and did it.

This all points to the need for flexibility, adaptability, and teamwork as circumstances change, often in unexpected ways, when managing material disruptions. It also points to the need for practice, such as scenario analyses and exercises, and learning from past experiences, not so much detailed specifics, but approaches and resilience, so people do not 'freeze'. Plans can never be counted upon in detail, but the process by which they are made and tested is essential preparation. Success when managing BNaU situations depends on the quality and commitment of both leadership and the people doing the work, and the strength

of their collective culture. These intangibles cannot be drafted into written processes, but they may dictate the level of success in BNaU situations.

Processes are typically prepared to address BaU circumstances. When there is disruption, the BaU presumption fails, and so it may not make sense to continue trying to do what was done in BaU mode. The impact of the driver(s) of the BNaU situation needs to be recognised. Sometimes, in the name of efficiency, backups and redundancies are removed from processes. In BaU situations, this may work, but in BNaU situations, this can lead to breakdowns in the process chain that cannot be easily repaired. Separate BNaU processes or process adjustments may be needed.

Entities providing services need to establish their expected service level standards in both BaU and BNaU situations (especially for critical services), as well as identifying triggers for when situations move between BaU and BNaU. BaU service standards may not apply in BNaU situations, so entities need to manage their customers' expectations in BNaU situations. They should provide assurances that key services will be maintained in BNaU situations. This implies that entities should clearly communicate to their consumers how they intend to manage their BNAU situations. This also included identifying the key services covered and their BNAU service standards. A specific example of this might be setting the expectations around how promised regular streams of income will be provided, assuming the receiving bank or other financial institution can receive them (but the entity cannot control).

We emphasise this point as the entities have the opportunity before the BNaU situation occurs, and perhaps the obligation, to set service level expectations in both BaU and BNaU circumstances.

This also emphasises the need for entities to establish a Risk event register in which the progress of the risk events and their resolutions can be documented and then reviewed to extract lessons for the future. They also serve as references when similar risk events occur in the future.

2.4 Operational resilience

The BIS document 'Principles of Operational Resilience', see BIS 2021, was noted in the Introduction. This document outlines principles of operational resilience in a banking context.

Supervisors globally, including APRA, have recognised that these principles are applicable in all financial service domains, including banks, insurance, and superannuation.

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 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 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. This principle extends to so-called fourth parties, as third parties may depend on them for the delivery of components of critical services to them.
- **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 the 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 entity's critical operations.

This is an extensive canvas to paint operational resilience on. The 'success test' embedded in Principle 1 is important, as discussed below as a separate topic.

CPS230 and CPG230 give some high-level steps to take to implement operational resilience. They provide a high-level path to move from principles to their implementation.

The application of the success test is not specifically referred to.

The set of key steps for addressing operational resilience is summarised here:

1 **Govern and implement their strategy and approach** to operational resilience, operational risk, and operational risk events in a management framework, including reporting 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 their 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 risks to identify control weaknesses, 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.

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.

The path that resolutions of risk events may take can evolve over time, sometimes as a consequence of actions taken (or not taken). That is, the 'footprint' of risk events can often reflect multiple risks that may more conveniently or typically be considered in isolation when taking a prospective view. Operational risk events may occur in clusters since the stress of the first one may reduce the capacity to deal effectively with subsequent events. These could be termed as 'inconvenient truths', and we refer you back to the BNaU discussion above. The importance of corporate culture and corporate risk culture in the resolution of risk events and other identified issues was highlighted by the Hayne Royal Commission. The length of time taken for some of the issues identified as needing to be addressed to actually be addressed may be indicative of how entrenched some risk culture and corporate issues may be.

2.5 Success test: A new paradigm

The crucial learning to take from the operational resilience 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 processes or perspectives. It is about maintaining critical services to consumers during disruptions within specified tolerance levels.

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.

An impartial, if lagging, indicator of the status of the success test for customers in the financial services industry is Australian Financial Complaints Authority data. See AFCA 2024. Complaints against financial services providers are made for a range of reasons, most of which, but perhaps not all, will be relevant to operational resilience and operational risk in particular. For example, consequences of mis-selling (or perceived mis-selling) or inappropriate claims treatments. These complaints may not necessarily reflect the impact of disruptions on financial services providers, as they may be more indicative of overall poor or slow processes, quality of customer service, or inbuilt issues with a good customer service culture.

2.6 Scale of the challenge

The enormity of the costs of risk events in the financial services industry is highlighted by the APRA statistic, reported in its Response to submissions on CPG230 in 2024, that the ORX global banking database reported 65,000 loss events between 2016 and 2021 with total losses close to $ 600 billion, which speaks for itself.

More specifically, recently in Australia:

- The 2019 Hayne Royal Commission has highlighted significant systemic issues of significant size. While some may have been addressed, others continue to fester. The widespread issues around the timely payment of death benefits to members' beneficiaries by super funds are an example of this.
- In 2025, we have seen serious and possibly concerted hacking attacks on superannuation funds. The response of some of the known affected super funds has drawn criticism from security experts who have warned that cyber defences may be inadequate, from commentators who have suggested some government responses along the lines of 'cyber-attacks occur all the time' may represent a 'head in the sand' attitude, and a down-playing of the reported financial impacts of these attacks only representing a small proportion of total funds under management. The specific members whose life savings may have been compromised may feel that being averaged out is not an appropriate or sympathetic response. This may do little to

encourage public confidence in the current system or its will and capacity to address risk events of this sort of unanticipated but potentially individually catastrophic nature.

In terms of operational risk reserves held by financial institutions, recent APRA statistical reports show that the operational risk aggregate reserves in Australia for Superannuation funds exceed $50,000 million, General insurance about $2,500 million, and Life Insurance just over 1,000 million. These are significant numbers.

It is also salutary to remember that nearly 10 million customers had their confidential data stolen in each of the Optus and Medicare hacking attacks in 2022.

3 Managing a portfolio of risks

3.1 Risk event impact – frequency and severity

We assume that we are dealing with residual risks, not inherent risks. That is, risks that are assessed after the consequences of mitigation measures have been reflected. We also assume there is a Risk register in which inherent risks, mitigation measures, and resultant residual risks are recorded (amongst other things, such as responsibilities and criteria used for making assessments). We will also assume that risks listed in the Risk register can be seen as independent of each other; otherwise, if there are dependencies, there may be elements of 'double counting' to manage.

Including a risk in a Risk register should automatically mean it has been identified and considered. If not, there is the possibility that the Risk register is not being used as it should be and may be more of a 'tick-box' compliance exercise. Risks not included in a Risk register are either considered immaterial from the perspective of the Risk register and are addressed as part of standard business practices, or have not been identified. This highlights the importance of maintaining an up-to-date and effective Risk register. Unidentified risks when an instance of them occurs as a risk event are unexpected and unassessed. These are inherently BNaU events, and their treatment will necessarily be more ad hoc than when more standard processes can be applied. In these circumstances, there may be heavier reliance on the intrinsic capabilities of the people involved – alertness, flexibility, adaptability, teamwork, etc, as there may well not be established procedures to follow. Such competencies can be enhanced by using scenario testing.

The impact of risk events is often thought of in terms of two criteria, frequency and severity, with an overall impact being a reflection of the compound effect of both frequency and severity. It may be that frequency and/or severity assessments are estimates based on experience and judgement and may be subject to biases. Each risk's potential expected impact is then commonly represented by a point on a risk heat map. We use the word 'expected' to indicate we initially seek a 'best estimate' of impacts, but should remain aware that these estimates may be imprecise.

Even when mathematical models are constructed to provide insight, we should remember that the input data may be imprecise, which can impose unavoidable limitations on the reliability and/or precision of outputs.

It is useful to remember that a key purpose of this process is to generate transparent and reliable information that can be input into decision-making processes. It is not to 'make the decision' as other issues may be pertinent to the decision-making.

We leave aside the issue that both expected frequency and expected severity are one measure of underlying distributions, with another key measure of these distributions being a measure of variability, such as standard deviation.

We also leave aside the issue that the severity of a risk event may vary depending on the criterion used to assess it. While a dollar financial criterion is often used, other criteria may also be used, such as regulatory risk, reputational risk, or internal organisational and/or staff impacts. When multiple criteria may be applied, this raises the question of how to 'combine' them in some way to get an overall assessment which may depend on the perspective taken.

As the 'lens' severity is viewed through varies, the severity result may also vary. For example, reputational risk events may be considered to have a comparatively low immediate financial impact (excluding possible future business losses) but may aggregate in a more exponential manner rather than a linear one. That is, the first reputational risk event may be seen as having minimal severity, but the second or third one suddenly gets a lot of attention and has a much bigger impact, as it may be seen as symptomatic of deeper issues.

An example of how operational risk issues can leverage adverse results is that of the NAB rogue trading issue in 2004, which led to a highly critical APRA report and far-reaching reforms at NAB. See NAB 2004. Other more recent examples, following the Hayne Royal Commission, suggest that issues remain.

It is perhaps self-evident that the scales used to assess frequency and severity are entity dependent and reflect the entity's risk appetite and risk culture.

The risk heat map is a matrix with two dimensions, the frequency of a single event's expected occurrence and its expected severity given it has occurred. Often, these dimensions are categories rather than continuums. It is common for the dimensions to be split into 3, 4, or 5 categories or buckets.

A measure of risk appetite can then be imposed by determining which boxes in the matrix are 'acceptable' and which are not. The overall impact of a single risk event is then assessed by some combination of the frequency rating (bucket it is in) and the severity rating(bucket it is in). The impact is often computed by adding the two ratings, and sometimes by taking their product.

This can lead to prioritisation challenges when the expected impacts of multiple risk events are in the same box in the heat map. It can also lead to challenges when more the one box in the matrix has the same impact assessment.

In this context, note that the risk appetite assessment need not be symmetric, so some discretion is available when the risk appetite is being set.

This may look like the following, with the relevant cell chosen for a given risk:

Risk heat map for a single risk event

	Severity	Insignificant	Minor	Moderate	Major	Severe	Catastrophic
Likelihood		1	2	3	4	5	6
Almost Certain	5	Low	Moderate	High	Extreme	Extreme	Extreme
Likely	4	Low	Moderate	High	High	Extreme	Extreme
Possible	3	Low	Low	Moderate	High	High	Extreme
Unlikely	2	Low	Low	Low	Moderate	Moderate	High
Rare	1	Low	Low	Low	Low	Low	Moderate

Note the diagonal colouring to identify categories of risk impact rating. Actions taken for a particular risk depend on its risk impact rating.

The risk impact rating is used as part of the management process for the individual risk. For example:

Risk impact rating - actions

Risk Impact Rating	Risk Appetite	Assessment	Action Required
Low (1)	Accept/Monitor	Risk is acceptable or part of a deliberate strategy	Manage by routine procedures;
Moderate (2)	Mitigate	Entity willing to accept some risk and implement controls to manage within tolerances	Assess the risk; review adequacy of current controls
High (3)	Mitigate/Transfer	Entity may transfer part of the risk to a third party (eg insurance or reinsurance)	Risk to be given appropriate attention & demonstrably managed;
Extreme (4)	Transfer/ Avoid	Risk is unacceptable; entity to avoid	Immediate attention & response needed

Risk impact ratings are also used later as inputs to the risk aggregation process.

The use of a small number of buckets can be accused of being a rather 'blunt' approach. We remind you of the discussion above regarding the lack of precision and the risks of spurious accuracy. A small number of buckets has the advantages of being more accessible and relatively straightforward to apply.

We remind you that the key objective of this process is to provide insight and information for decision-making. It is not intended to be 'the answer' as other considerations may be pertinent to the decision-making.

3.2 Risk event velocity – leapers and creepers

Risk events can unfold quickly or slowly. If they unfold slowly, while they may still be significant, there is more time available to address them. The pace at which risk events unfold, given they occur, is often referred to as the risk (event) velocity. For those that unfold quickly, we use the term 'leapers', and for those that unfold more slowly, we use the term 'creepers'. Examples of leapers might be a hacking attack seeking data if detected while it is in progress or an attempted external fraud. Examples of creepers include incorrect fees being charged daily in a unit

pricing calculation or the consequences of very slow treatment of insurance death benefits by superannuation funds. Differing approaches may be needed for leapers and creepers to reflect their different time scales.

A way of differentiating the risk events in a specific frequency-severity box in the risk heat map matrix is to use a measure of expected risk event velocity. Each risk event is given a measure of its expected velocity, analogous to the frequency and severity ratings. An overall risk impact is then determined by combining the three ratings -frequency, severity, and velocity. As above, additive, multiplicative, or combined approaches can be taken. For more flexibility, the ratings may also be given weights. For example, velocity for a specific risk may be considered more important, so its velocity is given a higher weight than the other two. This approach reflects another aspect of a risk event and provides more discrimination. Conceptually, this approach has a three-dimensional array in which the risks are placed (reflecting their three assessments) in boxes rather than the more traditional two-dimensional matrix. In any case, a risk impact rating is determined and can then be taken forward.

3.3 Aggregate assessment of two risk assessments

From the perspective of managing a risk portfolio, which is a collection of individual risks, a challenge is to gain insight into the overall or aggregate behaviour of the portfolio. Management may naturally be interested in the behaviour of a single possible risk event that may be new and/or not under control, but they are also interested in the overall behaviour of the portfolio of risks. Portfolios do not behave as any one of their components, as illustrated by the common experience with investment portfolios when comparing the overall behaviour with the behaviour of the individual investments held in them. Management is likely to want to make decisions based on the information they can get on the expected behaviour of a risk portfolio in addition to the behaviour of some of its individual components. This provides a management tool that can be used to support more insightful decision-making. For example, different scenarios may be explored.

The core challenge in moving to an assessment of portfolio behaviour is forming an assessment of the aggregated risk that is the combination of two individual risks. Once two risks can be aggregated, it follows that three or more can then be aggregated by using a pairwise aggregation approach.

As when assessing the risk rating of a single risk, we noted that a key aim of this process is to generate transparent and reliable information that can be input into decision-making processes. This remains the case when aggregating two risks. As before, the aim is not to ‘make the decision’ but to inform the decision as other issues may be pertinent to the decision-making. As noted above, transparency and reliability come from a relatively straightforward process that can be applied in a structured way, is trusted, and can be flexibly applied to a range of options.

We assume we are looking at expected values of risk events, the risk events are independent of each other, and we are considering residual risk. Remember we are using the word ‘expected’ loosely, so not with precise mathematical meaning.

While extending mathematical analysis and financial model building to better reflect the distributions of risk event impacts may be considered, we do not pursue this path as it can very rapidly become complex and subject to spurious accuracy. Our intention is to provide a path that is accessible, can be applied and appreciated by a wide range of people, is robust, and can be applied as a decision-making input and management tool.

To combine the results for two separate risks into a single aggregate risk assessment, the results for the two input risks need to be comparable. We achieve this by using the risk impact ratings. See the picture near the end of section 3.1.

The risk impact rating provides a comparative scale to assess the importance of the risk relative to other risks. The risk impact rating is made up of categories rather than continuums and may be split into 3, 4, or 5 categories or buckets.

Using four buckets as an example, the risk impact rating is shown in the picture near the end of section 3.1.

Assigning a risk impact rating to an individual risk can be done in many ways and should reflect the purpose of the aggregation process. As noted above, we are not seeking to follow a mathematical/financial modelling path. Rather, we are seeking to assess a comfort level associated with the risk as reflected in the description of the risk impact rating with:

- Green representing 'comfortable'
- Yellow 'some discomfort but expect this to be managed'
- Orange 'discomfort that may be able to be managed' and
- Red ' not comfortable'

How we arrive at the chosen level of comfort can be flexible and reflect the perspective of the aggregation.

- If the assessment is based on a more qualitative process, then it may be more subjective. An example may be where the focus is on managing reputational risk. A potentially significant advantage of more qualitative approaches is that they can include a broader range of people with disparate skills and perspectives who then collectively and constructively pool their knowledge and experience. That is, the assessment is made through a structured consensus from a group of experts. This is an example of 'collective intelligence'[2] and, when structured, is often called a Delphi process.

  This has the advantages of being inclusive and accessible, combining perspectives from both qualitative and quantitative perspectives, and

[2] For those who may doubt the validity of 'collective intelligence', reflect on the capacity of ants, who collectively are sophisticated in their farming of aphids (but individually are not so smart), bees with their sophisticated society and capacity to produce honey in hives, and, perhaps closer to 'home', the value of effective professional peer review. There are many business examples that demonstrate the power of applying collective intelligence approaches.

reducing the impacts of individual biases, potentially leading to more objective and robust group conclusions. It also provides a mechanism for acknowledging, but not being curtailed by, some of the inherent uncertainties involved when making assessments.

The Delphi approach is well established as being able to support consensus building, ownership, and good decisions (often better than those made by individuals, no matter how skilled they are). Such assessments can be made in a structured way and recorded for future review. It takes a broader perspective and can be very effective when some of the issues are not amenable to numerical quantification.

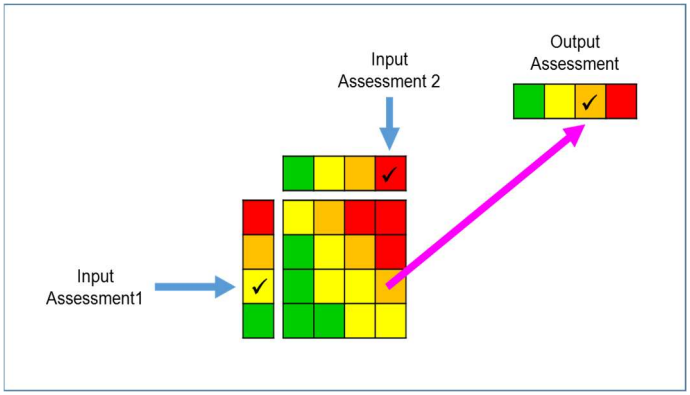
- If there is a more quantitative focus, for example, financial, then the assessment may reflect modelling or estimates of expected costs. This presumes that the required modelling can be done, so in some cases may have limitations. Model outcomes may also be attributed false precision as the distributions etc applied may reflect imprecise or incomplete data, leading to inherent limitations of outputs. As noted above, there may be subjective judgements and biases involved when more mathematical parameters are decided on.

The scale for the risk impact rating is then used as the axes for a risk aggregation heat map. The boxes in the risk aggregation heat map, the outputs, are restricted to be chosen from the same scale as used for the risk impact rating. The structure of the boxes in the risk aggregation heat map is flexible and can be tailored to suit the purpose of the aggregation process and the stage of the aggregation process. For example, an aggregation focusing on reputational risk may look quite different to one with another focus.

The output is then a risk impact rating for the aggregated risk that is carried forward.

The process, using a hypothetical risk aggregation heat map, is illustrated below.

Risk aggregation heat map

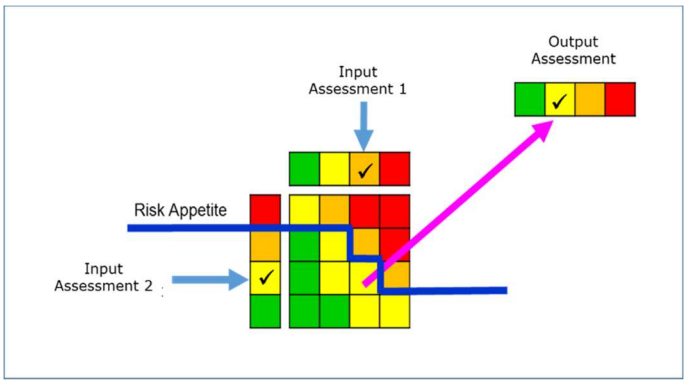


The process for aggregating two risks can be applied iteratively in a tailored and structured way. For example, applied with the inputs being the output from the first aggregation and the result from a third risk event assessment.

An important implementation step is to include a risk appetite over the risk aggregation heatmap. This means that an assessment of whether the aggregate

risk rating is inside or outside the risk appetite. Pictorially, this can be shown by a line that follows a chosen set of boundaries in the risk aggregation matrix.

Risk aggregation heat map with risk appetite



The output risk assessment obtained from a risk aggregation may be scaled (most likely down) when it is moved up to be a higher level input in the aggregation process to reflect the scope at the higher level being broader than at the lower level. Such scale factors should be determined before making the actual aggregations. Note that without making explicit assumptions about these scaling factors, the implicit assumption is that they are all the same (say with a value of 1).

To reduce the risk of 'backfitting' choices of risk aggregation heat maps should preferably be made, documented, and justified before the risk impacts are fed through them. Review may lead to adjustments, but then these adjustments should also be documented and justified.

A natural question that arises is about the order in which risks are aggregated and whether this makes a difference to the overall portfolio outcome.

From a mathematical perspective, if true expected values are being used, the final portfolio outcome will be indifferent to the order in which (expected) risk impacts are aggregated, since the expected value of the sum of random variables is the sum of their expected values. In practice, we are not generally dealing with exact expected values (see the above discussions on imprecision and estimation), and it is more natural to group risks into similar categories and then develop sub-portfolios, which are then aggregated. This permits sub-portfolios for (say) departments, then divisions etc, to be constructed as part of an overall entity portfolio risk aggregation. There is also flexibility in determining the scale factors applied to risks and aggregated risks as they move up through the aggregation process.

When it comes to detailed implementation, it is possible to refine the aggregation process by adding some more input information for the buckets on the axes of the risk aggregation heat map. This information reflects how full the input bucket is and uses a sub-bucket approach. That is, carrying an assessment along the lines of 'slightly full', 'medium full' or 'mostly full' forward. This can be reflected when the structures of risk aggregation heat maps are specified. This can be well structured, but we reiterate our warnings about the 'rabbit hole' of spurious accuracy and the need for process accessibility and transparency.

At this point, it is important to remember that the focus is more on assessing changes in outcomes than on the exactness of the specific outcomes. That is, it is a focus on trends rather than absolute outcomes. The question of 'are we doing better or worse than before at an aggregate (portfolio) level' can then be addressed over time. As long as the processes used are comparative, the absolute value of the outcomes may not be significant, but their movement is. This can provide a valuable management tool as varying scenarios can be considered and compared.

3.4 Level of precision and reporting

It is perhaps important not to get overly prescriptive or seek too much precision in this process. Some inputs to the process may be 'woolly' and/or subjective, and there is then no point in trying to get precise outcomes from imprecise inputs, with the risk of spurious 'accuracy' and perhaps generating false confidence. The key focus is on getting an indication of the relative impact of the risk events. This is a different thing to seeking measures of their absolute impacts. Having a view on relative impacts can then inform further discussion and analysis to support business decisions regarding further priorities and actions. That is, the outputs from risk heat and risk aggregation heat maps are inputs to a broader business decision-making process. This business decision-making process may well also reflect other inputs.

Commonly, these individual assessments are each reported using some form of 'traffic light' approach. If three 'traffic lights', red, amber, and green, are used, three categories of acceptability are specified, and each expected risk impacts are reported accordingly. Typically, red represents unacceptable, amber is ambivalent, and green is acceptable. This approach has the virtue of simplicity, but it can also be quite blunt, as any movement within the traffic light colours may not be reported. A finer gradation could be used (such as five 'traffic' lights), but note the comments above about assessing priorities as inputs for further discussions and the need to avoid spurious precision.

The success of operational resilience policies, frameworks, and processes depends on the quality of Board governance, senior management leadership, and the strength and maturity of the entity's culture and risk culture. Ultimately, while tools and information can be provided, it is how these tools are used and the quality of the people assessing these inputs and making decisions that will determine success. Strong integration into the overall ERM framework is also important.

The pervasive nature of operational risk and operational resilience, underpinning all activities, makes their risk maturity and contribution their effective management delivers to overall ERM success a key to long-term entity success.

The focus of this paper is on developing processes for assessing the expected impacts of operational risk and resilience events. We noted above the scale of the challenge and the level of funds held in operational risk reserves. As experience develops, the links between operational risk reserves, the drawdowns from them,

and their management should be considered. In this context, for superannuation, APRA's revised SPS114 and SPG114 should be considered.

3.5 Prospective risk identification

Risk registers and Risk event registers focus on identified (future) risks and identified (past) risk events and near misses.

A proactive approach to identifying new and emerging risks, which may need a higher priority than previously assessed, supports maintaining the currency of the risk register. The emergence of cyber risks over the last decade is a good example of this. Others include the challenges with AI applications in general, more specifically automated individual underwriting and claims management, and the impact of climate risk events on financial service entities, including the delivery of services relating to recent cyclones, floods, or bushfires.

A structured approach to regularly scan the environment for new and emerging risks and to reprioritise previously identified risks may help future-proof entities. As risks are better understood, they can progress from the environmental scan to the Risk register.

3.6 Silos

Implementing CPS230 and managing its implications is not taking place in regulatory silo.

APRA has long had a focus on financial resilience with its suite of capital standards covering a range of requirements, including Operational Risk (see CPG110 et al) and guidance on other topics, including Climate Change Financial Risks (CPG229), Financial Contingency Planning (CPS190), and Resolution Planning (CPS900). APRA introduced the idea of operational resilience some time ago. See, for example, the wider context described in APRA's Supervisory Review and Intensity Model, SRI 2020.

CPS230 now consolidates and streamlines several prudential standards and their related guidance into one place. These include standards on Business Continuity (CPS232), Information Security (CPS234), Pandemic Planning (CPS233), and Outsourcing (CPS231).

There are multiple interactions between CPS230 and other APRA initiatives. CPS230 and CPG230 refer directly to some of them, including Risk Management (CPS220 and SPS220), Operational Risk Financial Requirements (SPS114), Fit and Proper Requirements (CPS520 and SPS520), and others already mentioned above.

APRA's program of regulatory and supervisory objectives should be viewed as an interrelated whole rather than a set of independent initiatives.

3.7 Systemic operational resilience and risk

The discussion in CPS230 and CPG230 implicitly assumes a single entity focus. An underlying implication of this is that the other entities in a sector remain in BaU mode when the entity in question enters BNaU mode due to a (material) risk event. This may be inappropriate for a range of reasons, including:

- A third (or fourth) party provider that is a major player or even a monopoly supplier, having a material operational risk event that impacts multiple regulated entities. The regulated entities remain responsible to their customers for the maintenance of critical services to them. In this regard, consider the current concentration of administration services for superannuation funds.
- The potential impacts of groupthink or complacency amongst entities in particular financial service sectors. This might arise when the talent pool is small, concentrated, and may not be as open to less traditional newcomers who may not have 'served their time' as they might be. Some of the findings of the Hayne Royal Commission might be in this category.
- External events that have a systemic impact. Entities have no control over the occurrence or progress of the event, but they still need to address its consequences for them and their customers. Stock market crashes are an obvious example. The current global turbulence due to the significant US tariffs is a current example. If there is sufficient turbulence in the investment markets that valuations cannot be made with reasonable confidence, then unit pricing may not be able to be reliably struck, inhibiting or preventing redemptions and/or deposits from unitised investment funds - inside and outside the superannuation system. This has occurred in the past and so might occur again. Pandemics, which may have more diverse, pervasive, and unexpected impacts, both financial and more broadly, are another topical example.
- The extent of coverage of the population. APRA has suggested that the Australian insurance sectors may not be as systemically important as banking and superannuation, as its proposed 'system-wide' stress test is expected to focus on banking and superannuation. It is also the case that the total assets of life insurers and general insurers (and health insurers) are each much smaller than the total assets of the banks and the superannuation system. In 2021, www.theglobaleconomy.com reported that over 99% of the Australian population held a bank account. In 2019, APRA reported that over 78% of the Australian population held superannuation. Recently, the Noble Oak Pulse survey reported that 60% of the Australian population held a life insurance policy, 89% held house and contents insurance, 80% held health insurance, and 78% held contents insurance. APRA also reports that at 30 September 2024, about 55% of the population held a general treatment health insurance product (and 45% held a hospital cover). Services that are used by a large proportion of the population may be systemic due to the breadth of their coverage. While there are many aspects to the failure of HIH in March 2001 (and a Royal Commission), remember that the withdrawal of the HIH insurance services had materially adverse systemic impacts.

A systemic consideration is built into the discussion of identifying critical services and the operational resilience tolerances that an entity is expected to set. Note the final clause in CPS 230 paragraph 35:

> *Critical operations are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system.*

It is interesting to review APRA's actions and responses to the COVID 19 pandemic. They are pervasive, varied, and tailored to the various financial service sectors. See the APRA document COVID 19. The conclusion seems to be that, due to prior preparation and resilience capacity building, the Australian financial services demonstrated strong resilience during the pandemic. The COVID 19 pandemic was a global event as well as a systemic event globally and in Australia. Its impacts were, and in some cases continue to be, widespread. Also, in many cases, impacts may be unexpected, leveraged, and continue to have repercussions in many areas today.

Looking forward, APRA has indicated they intend to conduct a system-wide stress test, focused on banks and super funds, later in 2025. This reflects increasing concerns about the increasing levels of interconnectivity and possible impacts of system-wide dynamics that are not always well understood and may be unexpected. These impacts impinge on individual entities in ways perhaps outside their direct control. The comments above regarding the concentration of third-party service providers are an example of this. Another example is APRA's flagged concerns around the liquidity of superannuation funds in possible BNaU circumstances.

4 Operational resilience survey

PFS has initiated an industry-wide survey on operational resilience and CPS230 progress. The objective is to track the progress of the operational resilience journey and develop an operational risk event database. CPS230 applies without distinction in all regulated financial services entities, life, general and health insurance, superannuation, and approved deposit-taking institutions. However, the operational resilience journeys may vary between sectors and within sectors. This may support cross-fertilisation of ideas and approaches. CPS230 also notes that the approach entities take to CPS230 should appropriately reflect their size, business mix, and complexity. This 'proportionality' discussion will develop over time, and more clarity can be expected to evolve. For example, regarding what actions and steps need to be undertaken by all players in all cases.

The intent is to conduct this survey annually. Point-in-time assessments are useful, but progress can be better assessed by reviewing trends. Also, annual surveys permit new topics to be included.

The first survey has focused on life insurers (including Friendly societies), general insurers, and superannuation entities. Extensions to include approved deposit institutions and health insurers are planned for the future.

The results and analysis of the initial PFS Survey are expected to be reported on separately, both in aggregate and in more detail to participants.

This continues from preliminary work previously published. See PFS 2024.

5 Key messages

Operational resilience takes a broader perspective than operational risk management, while including operational risk. A core requirement of operational resilience is the obligation to maintain critical services, subject to tolerance levels, to customers through disruptions. It therefore has an outward-focused and externally oriented 'success test' of whether these critical services are maintained to an acceptable standard when the provider experiences disruptions, in a Business Not as Usual situation. This requirement of CPS230 reflects a paradigm shift in how operational resilience and operational risk-related issues are expected to be managed.

Meeting the requirements of CPS230 begins the journey for developing operational resilience, and some building blocks should already be in place. These requirements provide a minimal set of objectives to be met. Complying with CPS230 is a necessary foundation step, but it is not sufficient for success. Good practice will develop over time and can be expected to set higher standards of practice. As this journey progresses, risk culture and risk maturity can be expected to improve, contributing to improving ERM. The sufficient conditions for success focus on leadership, culture, and risk maturity. Leadership will come from boards and senior management as they own, set, and implement clear policies and oversee process improvements. In this context, managing operational resilience can be seen as an opportunity with benefits beyond compliance on offer. Improved efficiency and robustness from integrated reviews, streamlining and improving processes, as well as improving customer experiences and, hopefully, trust.

Operational risk and resilience address a broad spectrum of risks. We provide an approach that allows aggregate assessments over a risk portfolio and an assessment against risk appetites to be made. This structured approach relies on the adequacy of the Risk register. This approach is flexible, robust, inclusive, and broad-based as it can reflect both quantitative and qualitative assessments that can be inputs into wider business decision-making processes. This approach can generate summary perspectives, for management purposes, as distinct from getting a (long) list of individual assessments for individual risks. While we may not be able to slay the operational resilience and risk hydra, as risk will not disappear, we can hope to better understand it, mitigate and manage its impacts, and learn for the future.

An industry-wide survey has been initiated by PFS to assess progress along the operational resilience path. The intent is to conduct this survey annually. Point-in-time assessments are useful, but progress can be better assessed by reviewing trends. Annual surveys also permit new topics to be included. It is one thing to design systems, but it can be a bigger challenge to effectively implement and embed them to reap the benefits available.

Acknowledgements

Feedback and review from colleagues, including John Newman, Phil Stott, Madeleine Mattera, and Sean Williamson, have been welcome and helped improve this paper. Any errors in this paper remain my responsibility.

Author details

Jules Gribble, PhD FIAA CERA GAICD, is a Principal at PFS Consulting, based in Adelaide, South Australia. Jules can be contacted by:

✉: JulesGribble@PFSConsulting.com.au

✆: +61 456 801 401

🌐: www.PFSConsulting.com.au

References

AFCA 2024. *'AFCA Annual Review 2023-24'*, Australian Financial Complaints Authority, 0ctober2024.
See https://www.afca.org.au/about-afca/annual-review

COVID 19. 'COVID-19: A real-world test of operational resilience', APRA, APRA insights, 2020, Vol 3.
See https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience

CPS230. 'APRA Prudential Standard: CPS 230 Operational Risk Management', July 2025.
See https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf

CPG230. 'APRA Prudential Practice Guide: CPG230 Operational Risk Management', June 2024.
See https://www.apra.gov.au/sites/default/files/2024-06/Prudential%20Practice%20Guide%20CPG%20230%20Operational%20Risk%20Management.pdf

BIS 2021. 'Principles of Operational Resilience', Basel Committee on Banking Supervision, March 2021.
` See https://www.bis.org/bcbs/publ/d516.htm

IIF 2024. 'The Operational Resilience Ecosystem', M Boer and K Rismanchi, IIF Staff paper, December 2024.
See https://www.iif.com/Publications/ID/5987/IIF-Staff-Paper-Operational-Resilience-A-Brief-History-and-the-Road-Ahead

NAB 2004. 'Report into Irregular Currency Options Trading at the National Australia Bank', APRA, March 2004.
See (taken from ASX website following NAB publicly releasing it)
https://announcements.asx.com.au/asxpdf/20040324/pdf/3l25wl1595lng.pdf

ORX 2024. 'Annual Insurance Loss Report', O.R.X., June 2024.
See https://orx.org/hubfs/Website/Resources/Public%20reports/2024/ORX%20Insurance%20Operational%20Risk%20Loss%20Data%20Summary%20Report%202024.pdf?hsCtaTracking=f4327ff1-6aec-4bdf-807f-c733d05aac14%7C199d567b-cf21-487b-93f8-f0f29d024b01

PFS 2024. 'CPS 230 Check in: How does your progress stack up?', PFS, August 2024.
See https://pfsconsulting.com.au/wp-content/uploads/2024/08/CPS-230-Check-in-How-does-your-progress-stack-up.pdf

PFS 2023a. 'Operational Resilience: A bigger game and a broader perspective. How will you exploit this opportunity?', PFS, December 2023.
See https://pfsconsulting.com.au/2023/12/11/operational-resilience-a-bigger-game-and-a-broader-perspective/

PFS 2023b. 'Operational Risk Management Top Tips on CPS230', PFS, August 2023.
See https://pfsconsulting.com.au/2023/10/10/operational-risk-management-top-tips-on-cps230/

PFS 2022. *'CPS230 The Journey Toward Resilience and Adding Value. APRA's New Standard on Operational Risk Management'*, PFS, October 2022.
See https://pfsconsulting.com.au/2022/10/06/cps-230-the-journey-towards-resilience/

SRI 2020. *'Guide: Supervision Risk and Intensity Model',* APRA, October 2000.
See https://www.apra.gov.au/sites/default/files/%5Bdate%3Acustom%3AY%5D-%5Bdate%3Acustom%3Am%5D/Supervision%20Risk%20and%20Intensity%20Model%20Guide.pdf

Actuarial Outreach: Taming the Operational Resilience Hydra

Jules Gribble

2025