



DISCUSSION PAPER

Strengthening operational risk management

July 2022

Disclaimer Text

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© Australian Prudential Regulation Authority (APRA)

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence (CCBY 3.0). This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that APRA endorses you or your work. To view a full copy of the terms of this licence, visit <https://creativecommons.org/licenses/by/3.0/au/>

Contents

Executive summary	4
Glossary	8
Chapter 1 - Strengthening operational risk management	10
Chapter 2 - Operational risk	18
Chapter 3 - Business continuity	21
Chapter 4 - Service providers	25
Chapter 5 - Consultation and next steps	28
Attachment A: Policy options	30

Executive summary

Events of recent years have demonstrated the critical importance of financial institutions being able to manage and respond to operational risks, evident for example in the challenges of the COVID-19 pandemic, technology risks and natural disasters. Sound operational risk management is fundamental to financial safety and system stability.

To ensure that all APRA-regulated entities in Australia are well placed to manage operational risk and respond to business disruptions when they inevitably occur, APRA is consulting on a new prudential standard for operational risk management.

Objectives

The proposed new standard for operational risk management, which will replace and supersede a number of existing standards in this area, encompasses operational risk controls and monitoring, business continuity planning and the management of third-party service providers.

The aim of the standard is to:

- ***strengthen operational risk management*** with new requirements to address weaknesses that have been identified in existing practices of APRA-regulated entities. This includes requirements to maintain and test internal controls to ensure they are effective in managing key operational risks.
- ***improve business continuity planning*** to ensure that APRA-regulated entities are ready to respond to severe business disruptions, and maintain critical operations such as payments, settlements, fund administration and claims processing. It is important that all APRA-regulated entities are able to adapt processes and systems to continue to operate in the event of a disruption and set clear tolerances for the maximum level of disruption they are willing to accept for critical operations.
- ***enhance third-party risk management*** by extending requirements to cover all material service providers that APRA-regulated entities rely upon for critical operations or that expose them to material operational risk, rather than just those that have been outsourced.

The new standard is intended to ensure that APRA-regulated entities are well positioned to meet the challenges of rapid change in the industry and in technology more generally. In proposing a new prudential standard, APRA has also sought to streamline requirements with an outcomes-focused approach that brings together related operational risk concepts into a single standard.

Operational resilience

The proposed *Prudential Standard CPS 230 Operational Risk Management* (CPS 230) will replace five existing standards: *Prudential Standard CPS 231 Outsourcing* (CPS 231) and *Prudential Standard CPS 232 Business Continuity Management* (CPS 232) that apply to ADIs, life insurers and general insurers, the equivalent superannuation standards *Prudential Standard SPS 231 Outsourcing* (SPS 231) and *Prudential Standard SPS 232 Business Continuity Management* (SPS 232) and the private health insurance standard *Prudential Standard HPS 231 Outsourcing* (HPS 231). A summary of the new standard is presented in the graphic below.

Strengthening operational resilience



Objectives



Improve operational risk practices through enhanced focus of Boards and senior management



Minimising the impact of disruptions to customers and the financial system

Key features

CPS 230 Operational Risk Management

- Entities must manage operational risks with effective internal controls, monitoring and remediation
- Entities must be able to respond to disruptions and maintain continuity of critical operations
- Entities must understand and manage the risks from the use of service providers

Key outcomes for the community



Prepared

Identifying and effectively managing and responding to operational risk events reduces the impact of such events



Protected

Disruptions and their associated impacts will be minimised through robust business continuity planning



Resilient

Entities can continue to operate through disruption and provide key services to customers

Implementation

Existing standards until 31 Dec 2023

CPS 231
CPS 232
CPS 234
HPS 231
SPS 231
SPS 232

Standards from 1 Jan 2024

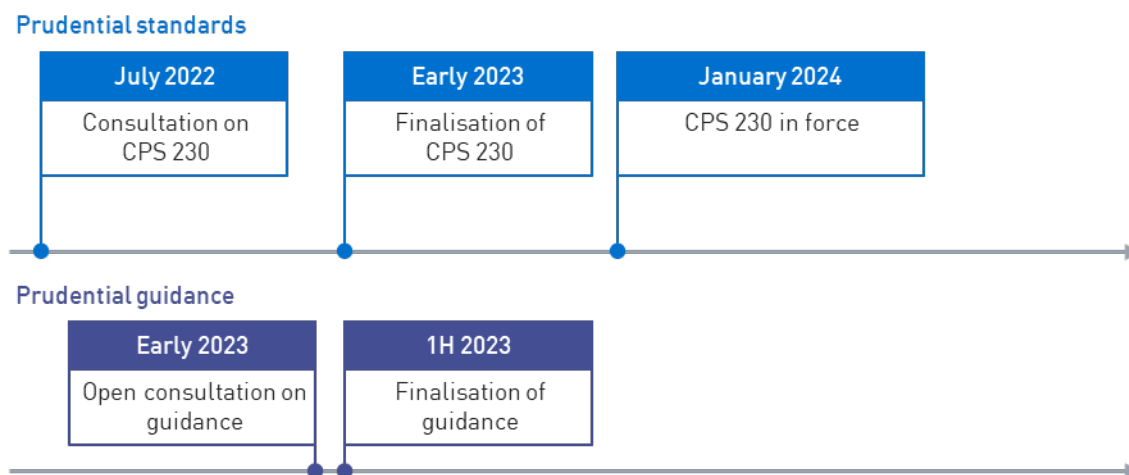
CPS 230
CPS 234

APRA intends to consult on guidance early in 2023.

Next steps

APRA welcomes responses to this consultation on the draft CPS 230 by 21 October 2022. Following review of feedback and submissions, APRA plans to finalise the standard in early 2023 and release draft guidance for consultation. As outlined in the intended timeline below, CPS 230 would come into effect for all APRA-regulated entities from 1 January 2024.

Figure 1. Timeline



Glossary

ADI	Authorised deposit-taking institution
APRA	Australian Prudential Regulation Authority
BaaS	Banking as a Service
BCP	Business continuity plan
Board	Board of directors of an institution or, for an RSE licensee, the Board of directors or group of individual trustees of an RSE licensee, as applicable
CPG 231	<i>Prudential Practice Guide CPG 231 Outsourcing</i>
CPG 233	<i>Prudential Practice Guide CPG 233 Pandemic Planning</i>
CPG 234	<i>Prudential Practice Guide CPG 234 Information Security</i>
CPG 235	<i>Prudential Practice Guide CPG 235 Managing Data Risk</i>
CPS 220	<i>Prudential Standard CPS 220 Risk Management</i>
CPS 230	<i>Prudential Standard CPS 230 Operational Risk Management</i>
CPS 231	<i>Prudential Standard 231 Outsourcing</i>
CPS 232	<i>Prudential Standard CPS 232 Business Continuity Management</i>
CPS 234	<i>Prudential Standard 234 Information Security</i>
HPS 231	<i>Prudential Standard HPS 231 Outsourcing</i>
Non-SFI	Non-significant financial institution
RSE	Registrable superannuation entity

RSE licensee	Registrable superannuation entity licensee as defined in s.10(1) of the <i>Superannuation Industry (Supervision) Act 1993</i>
SFI	Significant financial institution
SPG 223	<i>Prudential Practice Guide SPG 223 Fraud Risk Management</i>
SPG 231	<i>Prudential Practice Guide SPG 231 Outsourcing</i>
SPG 232	<i>Prudential Practice Guide SPG 232 Business Continuity Management</i>
SPS 114	<i>Prudential Standard SPS 114 Operational Risk Financial Requirements</i>
SPS 220	<i>Prudential Standard SPS 220 Risk Management</i>
SPS 231	<i>Prudential Standard SPS 231 Outsourcing</i>
SPS 232	<i>Prudential Standard SPS 232 Business Continuity Management</i>

Chapter 1 - Strengthening operational risk management

Operational risk management: a core foundation

The management of operational risk is an important foundation for financial safety and system stability. In APRA's overarching standards for risk management, *Prudential Standard CPS 220 Risk Management* (CPS 220) and *Prudential Standard SPS 220 Risk Management* (SPS 220), operational risk is defined as one of the core risks that all APRA-regulated entities must manage effectively.¹



Operational risk

Operational risks are risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events.

Operational risk is inherent in all products, activities, processes and systems. It includes legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk and change management risk.

Operational risk events can result in direct financial losses to an entity and may also compromise the entity's ability to continue to provide critical operations and services for customers. In extreme cases it could lead to entity failure.



Operational resilience

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

This involves:

- to the extent practicable, preventing disruption to critical operations;
- adapting processes and systems to continue to operate in the event of a disruption; and
- returning to normal operations promptly after a disruption is over.

Setting and maintaining appropriate standards for conduct and compliance are key components of effective operational risk management, as conduct and compliance breaches

¹ The other material risks defined in CPS 220 are credit risk, market and investment risk, liquidity risk, insurance risk and strategic risk. For an RSE licensee, the other material risks defined in SPS 220 are governance risk, investment governance risk, liquidity risk, insurance risk and strategic and tactical risks.

are often indicative of underlying failings in internal controls. Conduct and compliance breaches are typically categorised as operational risk events, as they are often associated with legal costs, regulatory penalties or regulator-imposed restrictions.² In maintaining appropriate standards for conduct and compliance, APRA-regulated entities need, amongst other things, to have robust processes and controls in place to ensure they comply with conduct regulation administered by ASIC.

Challenges in managing operational risk

The importance of operational risk management has been highlighted repeatedly in recent years, with regular examples of operational risk events and failures that have had both financial and non-financial implications.

APRA has observed three key trends in recent years:

- ***Control failures:*** While some operational risk events have been due to circumstances beyond the control of the industry, such as the COVID-19 pandemic, many others have arisen due to ineffective controls. To address these, APRA has taken action across a range of entities in the form of Court-enforceable undertakings, requirements for large-scale remediation programmes and the application of additional operational risk capital requirements.
- ***Low tolerance for disruptions:*** Disruptions to business operations, and to services offered by APRA-regulated entities, have the potential to impact key stakeholders reliant on real-time transactions and consistent availability. Depositors, policyholders, fund members and other customers have a low tolerance for disruptions, given the importance of core financial services in everyday life and an expectation that services will always be available.
- ***Increasing reliance on service providers:*** APRA-regulated entities are increasingly reliant on the use of service providers to support their business operations. Entities are looking to external providers not only for current in-house services ('outsourcing'), but also for new services, capabilities and expertise that extend their offerings to the market. Problems in service providers can quickly impact on the availability and level of service of an APRA-regulated entity, with flow-on impacts to the broader financial system. The expanded use of service providers is giving rise to longer and more complex supply chains, often involving a reliance on fourth parties and other downstream providers. The growing use of cloud-based services is one example of this trend.

Against the backdrop of these three key trends, APRA is proposing to introduce new and enhanced requirements to strengthen the management of operational risk and raise standards to align with the expectations and needs of the financial system and digital economy.

² See also <https://www.apra.gov.au/news-and-publications/how-to-manage-compliance-risk-and-stay-out-of-headlines>

Proposed changes to the prudential framework

The current components of the prudential framework for operational resilience are set out in the table below. Operational risk requirements have been articulated through overarching risk management principles set out in CPS 220 and SPS 220. To support this, there are specific prudential standards on outsourcing and business continuity management. In 2019, APRA released a new standard focused on information security, *Prudential Standard CPS 234 Information Security* (CPS 234).

In addition, there are several prudential practice guides (PPGs) targeting specific areas of operational risk. This guidance includes *Prudential Practice Guide SPG 223 Fraud Risk Management* (SPG 223) (for RSE licensees only), *Prudential Practice Guide CPG 233 Pandemic Planning* (CPG 233) and *Prudential Practice Guide CPG 235 Data Risk Management* (CPG 235).

Table 1. Current framework

Operational resilience	Prudential standard	Guidance
Operational risk management	<ul style="list-style-type: none"> Addressed at a high level in CPS 220 and SPS 220 	<ul style="list-style-type: none"> CPG 233 CPG 235 SPG 223
Outsourcing	<ul style="list-style-type: none"> CPS 231 HPS 231 SPS 231 	<ul style="list-style-type: none"> CPG 231 SPG 231
Business continuity management	<ul style="list-style-type: none"> CPS 232 SPS 232 	<ul style="list-style-type: none"> SPG 232
Information security	<ul style="list-style-type: none"> CPS 234 	<ul style="list-style-type: none"> CPG 234

The proposed framework for operational resilience brings together new requirements on operational risk management with updated requirements on outsourcing and business continuity into a single standard. This is consistent with APRA's strategic initiative to *Modernise the Prudential Architecture*, a multi-year programme that will improve the accessibility and adaptability of the framework, seeking to ensure that the prudential rules are easy to understand, find and navigate.

Table 2. Proposed new framework

Operational resilience	Prudential standard	Guidance
Operational risk management	<ul style="list-style-type: none"> CPS 230 	<ul style="list-style-type: none"> CPG 230 Pandemic planning (CPG 233) Data management (CPG 235) Fraud risk management - Superannuation only (SPG 223)
Information security	<ul style="list-style-type: none"> CPS 234 	<ul style="list-style-type: none"> CPG 234

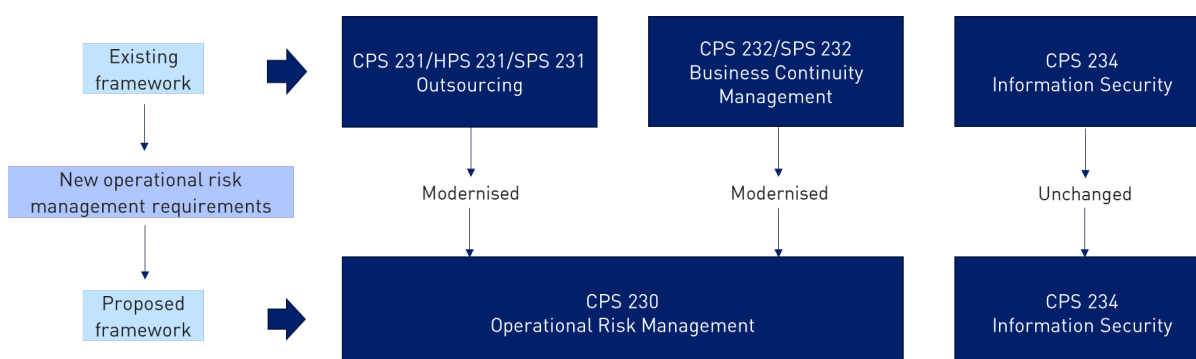
Development of operational risk management requirements

In developing CPS 230, APRA has adopted a principles-based approach with a focus on outcomes rather than process. In designing the new standard, APRA has had regard to:

- existing APRA standards for business continuity and outsourcing, which have been streamlined and updated;
- international standards, such as the Basel Committee on Banking Supervision’s *Core Principles*, and the recently released *Principles for Operational Resilience* and *Principles for the Sound Management of Operational Risk*;³ and
- international peer’s approaches and guidance, including the Prudential Regulation Authority (PRA) in the UK and the Office of the Superintendent of Financial Institutions (OSFI) in Canada.

APRA has also considered observations from its supervisory activities and reviews, and relevant findings from recent inquiries, including the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*.

Figure 2. Building blocks of the new standard



³ See [Core principles for effective banking supervision \[bis.org\]](https://www.bis.org), [Principles for operational resilience \[bis.org\]](https://www.bis.org), [Principles for the Sound Management of Operational Risk \[bis.org\]](https://www.bis.org)

Draft CPS 230 is focused on management practices for operational risk. APRA is not proposing changes to operational risk capital requirements for ADIs and insurers.⁴

RSE licensees must consider the extent to which operational risks could impact their business operations when determining their operational risk financial requirement (ORFR) target amount. APRA has recently consulted on the role of ORFR in strengthening financial resilience and will provide further information on the intersection between CPS 230 and the ORFR as these reforms progress in 2022.⁵



Proportionality

Setting prudential requirements that are not overly complex, relative to what is needed to ensure the financial safety and operational resilience of smaller entities, is an important priority for APRA. There are broadly two approaches to incorporating proportionality in the prudential framework, which are not mutually exclusive:

- One approach, which broadly applies across the prudential framework and has been embedded in the existing CPS 231 and CPS 232, is for all requirements to apply to all entities, but for entities to use their discretion to meet the requirements in a proportionate manner commensurate with the scale and complexity of their business. Such an approach may be supported by APRA guidance which explains how different types of entities might seek to comply with the expectations contained in the standard.
- The other approach is more explicit: APRA may completely exempt smaller, less complex entities that are deemed to be non-significant financial institutions (non-SFIs) from specific requirements. This approach has been applied in several cross-industry standards, including *Prudential Standard CPS 511 Remuneration* and the draft *Prudential Standard CPS 190 Financial Contingency Planning* (CPS 190). In the context of draft CPS 230, this could mean, for example, that requirements relating to documenting the processes for critical operations, scenario analysis and tolerance levels would only be applied to SFIs, and would be considered better practice rather than formal requirements for non-SFIs.

APRA would be particularly interested in the views of stakeholders concerning how best to achieve appropriate proportionality in the design and implementation of CPS 230, given the importance of sound operational risk management to all types of financial institutions.

⁴ For ADIs, these are set out in *Prudential Standard APS 115 Capital Adequacy: Standardised Measurement Approach to Operational Risk* (APS 115), which took effect on 1 January 2022. APS 115 applies to all ADIs from 1 January 2023, with the exception of non-SFIs. Non-SFI ADIs may apply a simplified approach to calculate capital (as set out in Attachment of A of APS 110 (2023)). For insurers, capital requirements are set out in *Prudential Standard GPS 118 Capital Adequacy Operational Risk Charge*, *Prudential Standard LPS 118 Capital Adequacy Operational Risk Charge* and the upcoming equivalent standard for Private Health Insurers.

⁵ Current requirements for the ORFR are set out in *Prudential Standard SPS 114 Operational Risk Financial Requirements* (SPS 114). Recognising the link between the ORFR and these broader operational risk reforms, draft CPS 230 notes that APRA may require an RSE licensee to meet an ORFR target amount determined by APRA under SPS 114. See <https://www.apra.gov.au/strengthening-financial-resilience-superannuation>

Overview of CPS 230

The overall aim of CPS 230 is to ensure that APRA-regulated entities are resilient to operational risks and potential disruptions. It requires entities to effectively manage their full range of operational risks, maintain critical operations through severe business disruptions and manage the risks arising from the use of service providers. An overview of the key requirements in draft CPS 230 is presented in the table below.

The key changes, relative to APRA's current standards, are new specific requirements for operational risk management, clearer definitions of critical operations and tolerance levels for business continuity and a broadening of the coverage of requirements from managing outsourcing to managing all service providers that the entity relies upon. These are further explained in the chapters that follow.

Table 3. Overview of draft CPS 230 requirements






Draft CPS 230	Key requirements
Operational risk management	<ul style="list-style-type: none"> • <i>Operational risk assessment</i> to ensure that APRA-regulated entities understand and monitor their risk profile • <i>Operational risk controls</i> which must be designed, implemented and embedded and regularly tested for effectiveness • <i>Operational risk incidents</i> which must be identified, escalated, recorded and addressed in a timely manner
Business continuity	<ul style="list-style-type: none"> • <i>Critical operations</i> which are processes that, if disrupted, would have a material adverse impact on depositors, policyholders, beneficiaries or other customers or financial system stability • <i>Tolerance levels</i> for the maximum disruption to critical operations that an entity would accept in a disruption, including the maximum time and extent of data loss • <i>Business continuity plan (BCP)</i> that sets out how the entity would manage and respond to a disruption to critical operations and must be subject to testing and review
Service provider management	<ul style="list-style-type: none"> • <i>Identification of material service providers</i> on which the entity relies for its critical operations or that expose it to material operational risk • <i>Service provider agreements</i> to ensure entities monitor and manage the risks associated with third parties and intra-group entities

Operational risk management should be integrated into an entity's overall risk management framework and processes, as set out in CPS 220 and SPS 220. Business continuity planning should also be consistent with, and not conflict or undermine, an entity's financial contingency planning, as required under CPS 190.

Balancing APRA’s objectives

The APRA Act requires APRA to balance the objectives of financial safety and efficiency, competition, contestability and competitive neutrality and, in balancing these objectives, promote financial stability in Australia.

APRA considers that, on balance, the proposals in this Discussion Paper will strengthen the resilience of the Australian financial system, improve financial safety and promote sound operations while not materially impacting on other regulatory considerations.

PRIMARY OBJECTIVES	
Financial safety 	Financial system stability 
<p>Improved: Financial safety will be enhanced by new requirements for operational risk management and updated requirements for business continuity and service provider management. Overall, these requirements will enhance both the operational and financial resilience of regulated entities, improving outcomes for depositors, policyholders and beneficiaries.</p>	<p>Improved: Financial system stability is expected to improve, with enhanced and updated requirements for the management of operational risk. In addition, enhanced business continuity planning will ensure regulated entities are well prepared for disruptions to their activities and able to minimise the impacts on critical operations.</p>
OTHER CONSIDERATIONS	
Efficiency 	<p>No material change: The proposals are not expected to materially impact on the efficiency of APRA-regulated entities, with no major impacts expected on competition, technology or innovation. APRA has acknowledged the importance of implementing the standard in a proportionate manner, and will use the consultation process to ascertain how that is best achieved.</p>
Competition 	<p>No change: APRA intends that CPS 230 will apply a proportionate approach, as with other standards and the prudential framework more broadly. The requirements are intended to apply commensurate with the size and complexity of an entity’s operations, and the extent of reliance on other parties for the provision of material services.</p>
Contestability 	<p>No change: The proposed requirements in CPS 230 largely reflect APRA’s existing supervisory expectations, and would not be expected to impede new market entrants or advantage new entrants.</p>

Competitive Neutrality



No change: The proposed standard would not create an advantage for public sector entities relative to other market participants.

Chapter 2 - Operational risk

The proposed requirements in draft CPS 230 are intended to establish a minimum set of expectations to ensure that APRA-regulated entities effectively identify, assess and manage operational risks.

The proposed requirements cover key areas where weaknesses have been observed by APRA in its supervision, as well as lessons learned internationally.

Draft CPS 230 places the onus on business-line management to take responsibility for the oversight and management of operational risk, embedded in the business rather than principally being the responsibility of risk management functions.

Strengthening oversight and management

Draft CPS 230 introduces a principles-based approach to operational risk management that is outcomes-focussed, and reflects that:

- the management of operational risk is foremost the responsibility of an APRA-regulated entity's business lines, and should therefore be embedded within the respective business;
- senior managers within the business are responsible for the ownership and management of operational risk across an entity's end-to-end processes; and
- the Board is ultimately accountable for the oversight of operational risk management, and is expected to ensure that senior management effectively implements and maintains the framework.

A key lesson from the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* was the importance of strong oversight of non-financial risks, with the Board having the relevant information to allow it to discharge its responsibilities and make informed decisions. Given this, and weaknesses identified by APRA as part of its supervision in recent years, draft CPS 230 specifically requires senior management to provide clear and comprehensive information to the Board on operational risk and maintain appropriate and effective information systems to monitor the operational risk profile.



Case study: Banking as a Service

Banking as a Service (BaaS) is a business model whereby an ADI provides third parties access to a technology platform, so they can allow their customers to utilise the ADI's banking services.

An ADI would need to ensure the BaaS arrangement meets the requirements in draft CPS 230, and that the operational resilience of the ADI would not be compromised, for example through money laundering, cyber-risk vulnerability or breaches of data confidentiality. This includes proposed specific requirements for an APRA-regulated entity to conduct a comprehensive risk assessment

before providing a material service to another party, to ensure that it can continue to meet its prudential obligations after entering the arrangement.

New products and activities

Draft CPS 230 requires an APRA-regulated entity to assess the impact of new products, services, geographies and technologies on its operational risk profile. New products or changes that materially alter the nature of a product offering typically impact an entity's operational risk profile and may require changes to controls and risk management processes.

Emerging technologies may result in novel operational risks for APRA-regulated entities. These risks need to be clearly understood, so that sound decisions are made and appropriate controls are put in place, together with robust management and monitoring.



Managing the operational risks associated with crypto-assets

Operational risks from activities and technologies associated with crypto-assets are an example of an emerging area where regulated entities will need to have prudent processes and controls. In April 2022, APRA wrote to regulated entities setting out initial risk management expectations for entities that engage in activities associated with crypto-assets.⁶ APRA noted that operational risk management is particularly important, and encompasses fraud, cyber, conduct, AML/CTF and technology risks.

APRA expects that all regulated entities will conduct appropriate due diligence and a comprehensive risk assessment before engaging in activities associated with crypto-assets, and apply robust risk management controls. In particular, draft CPS 230 would require an APRA-regulated entity to:

- ensure it assessed the impact of new products, services and technology on its operational risk profile;
- prudently manage arrangements with service providers, such as those that they may rely on in offering products associated with crypto-assets; and
- conduct business continuity exercises that would cover a range of scenarios, including potential disruptions to services provided by material service providers.

APRA is considering the appropriate prudential framework for crypto-assets in Australia in consultation with other regulators domestically and internationally. This will include requirements for credit, market, liquidity and other risks associated with crypto-assets. APRA plans to consult on draft requirements for ADIs following the conclusion of the Basel Committee's current *Consultation on the prudential treatment for crypto-asset exposures*, which will provide a starting point for prudential expectations for other APRA-regulated industries.

⁶ Refer to [Letter to industry - Crypto-assets risk management and policy expectations](#), APRA 21 April 2022

Internal controls

APRA-regulated entities should maintain internal controls to detect and manage operational risks within appetite. Given the criticality of the control environment to the management of operational risk, draft CPS 230 requires entities to ensure they maintain effective controls, commensurate with the size, business mix and complexity of their business activities.

APRA expects that internal controls would be sufficiently developed to effectively mitigate operational risks to within an entity's risk appetite and would be regularly reviewed and tested. Shortcomings and weaknesses identified in relation to internal controls would need to be rectified in a timely manner, to reduce the risk of a control failure at the point when it is most needed. A clear understanding of the end-to-end processes underpinning critical operations is also vital: it ensures an entity can identify its obligations, risks, required controls and necessary monitoring mechanisms, as well as understand the impact of business decisions on operational resilience.

Incident management

Draft CPS 230 would require an entity to ensure that operational risk incidents and near misses are identified, reported and addressed in a timely manner. Entities would also be required to notify APRA as soon as possible, and not later than within 72 hours of becoming aware of an operational risk incident that it determines to be material. These notifications are designed to ensure that APRA is informed of material operational risk incidents, and able to assess and respond to the potential for broader impacts on the financial system.

Chapter 3 - Business continuity

Draft CPS 230 incorporates and updates requirements for business continuity management that are currently set out in CPS 232 and SPS 232. This would require an APRA-regulated entity, to the extent practicable, to prevent disruption to critical operations, adapt processes and systems to continue to operate in the event of a disruption and return to normal operations promptly after a disruption is over.

Evolution in business continuity planning

CPS 232 was developed at a time when there was a focus on physical disruptions to businesses. This included, for example, the need to have back-up recovery sites to allow a business to continue to operate in some limited form. With the increasing move to digitisation, the focus of business continuity planning has shifted to maintaining critical operations and services for customers, including maintaining online capabilities.

Draft CPS 230 will formalise the need for entities to clearly identify their critical operations, set tolerances to define levels of disruption that would be unacceptable, and maintain credible plans to respond to and recover from incidents and events. Ultimately, draft CPS 230 seeks to minimise the likelihood and impact of disruptions on critical operations (including those where the entity is wholly or partially reliant on service providers).

Critical operations

Central to business continuity planning is the concept of 'critical operations'. These are activities and processes undertaken by an entity (or its service provider) which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, fund members or other customers or its role in the financial system.

The concept of critical operations in draft CPS 230 is similar to the existing concept of 'critical business operations' in the current CPS 232, but with a definition now more focused on outcomes and the key stakeholders of the entity rather than the entity itself.⁷ While it is the responsibility of the entity to define, identify and maintain a register of its critical operations under draft CPS 230, APRA has specified certain operations that must be included. This will ensure critical operations are consistently captured across the industry.

Draft CPS 230 requires certain operations to be classified as critical operations, as outlined below. There may be other operations that an entity undertakes that would also meet the definition of a critical operation.

⁷ 'Critical business operations' are currently defined in CPS 232 as the business functions, resources and infrastructure that may, if disrupted, have a material impact on the institution's business functions, reputation, profitability, depositors and/or policyholders.

Table 4. Specified critical operations

Banking	Insurance	Superannuation
Payments	Payments	Payments
Deposit-taking and management	Claims processing	Investment management
Custody, settlements and clearing	Customer enquiries	Fund administration
Customer enquiries		Customer enquiries

Critical operations are processes that would be important for a particular entity to ensure it could continue to deliver through a disruption. 'Critical functions', which may be determined as part of resolution planning, are services that are important for the financial system more broadly. The table below distinguishes the two concepts.

Table 5. Distinguishing concepts: Critical operations and critical functions

Distinguishing concepts	Critical operations	Critical functions
Prudential standard	CPS 230 Operational Risk Management	CPS 900 Resolution Planning
Definition	A process 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.	A function provided by an APRA-regulated entity that is important to financial system stability or the availability of essential financial services to a particular industry or community.
Focus	Entity-level	Financial system-level
Applies to	Defined by an entity as part of BCP, and maintained at all times	Determined by APRA on a case-by-case basis
Examples	<ul style="list-style-type: none"> • Deposit-taking and management • Payments • Custody • Settlements • Clearing • Customer enquiries 	<ul style="list-style-type: none"> • Very large deposit book

Tolerance levels

Under draft CPS 230, APRA-regulated entities would be required to set Board-approved tolerance levels for each of their critical operations. Draft CPS 230 specifies the nature of tolerance levels that must be set as:

- the maximum period of time an entity would tolerate a disruption to the operation;
- the maximum extent of data loss the entity would accept as a result of a disruption; and
- minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

The setting of tolerance levels is intended to be customer and outcomes-focussed; it is these factors that an entity would be expected to have front-of-mind when determining tolerance levels for critical operations. APRA may also set tolerance levels in circumstances where there are heightened risks or material weaknesses, including at a system level.⁸



Examples of tolerance levels

For payments, an entity may set tolerance levels for a disruption measured in hours or days. This may depend on the type of payment service and the granularity of the level. Tolerance levels are akin to a risk appetite for disruption and should be clearly justified and subject to challenge and review.

APRA expects that entities will set and regularly reassess tolerance levels, as they learn lessons from actual disruptions, testing and the development of industry practices. In the UK, a recent review of tolerance levels for payments revealed a wide range: from one working day for some payment processes to 24 hours to two weeks for others.⁹

Business continuity plan

As with the requirements under existing CPS 232 and SPS 232 to maintain a business continuity plan (BCP), draft CPS 230 also requires an APRA-regulated entity to maintain a BCP for its critical operations. The BCP must set out how the entity would recover critical operations within tolerance levels in the event of a severe but plausible disruption.

While draft CPS 230 sets out the key matters that a BCP must address, an APRA-regulated entity is responsible for ensuring its BCP is fit-for-purpose and is sufficiently comprehensive to be useful in appropriately responding to a disruption. The nature, complexity and size of an

⁸ As part of CPS 232, APRA-regulated entities are currently required to set recovery objectives: pre-defined goals for recovering critical business operations to a specified level of service within a defined period following a disruption. Tolerance levels are a similar concept, but have been updated to specifically include data loss. Draft CPS 230 also clarifies that APRA expects an entity to maintain critical operations within tolerance levels, rather than these just being an implicit part of business continuity planning.

⁹ [Operational resilience: next steps on the PRA's supervisory roadmap](#) PRA, 28 April 2022.

entity's operations are key considerations in the development and maintenance of a BCP. While draft CPS 230 is framed in the context of a single BCP, this does not prevent an entity from having multiple BCPs with, for example, detailed plans for each critical operation.

Testing and review

Draft CPS 230 requires an APRA-regulated entity to have a systemic testing program for its BCP that covers all critical operations and includes an annual business continuity exercise. The testing program would be tailored to cover the material risks of the entity and include a range of severe but plausible scenarios that could impact its critical operations. Such exercises would test the overall effectiveness of an entity's BCP and the entity's ability to maintain essential business operations within tolerance levels. The testing requirement is intended to highlight any deficiencies with an entity's BCP so that it is properly prepared should an actual disruption occur.

Draft CPS 230 includes audit requirements, as currently set out in CPS 232 and SPS 232. An APRA-regulated entity would also be required to submit its BCP to APRA on an annual basis, and notify APRA as soon as possible, and no later than 24 hours, of a material disruption to a critical operation or if it has activated its BCP. The notification would cover the nature of the disruption, the action being taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations.

Chapter 4 - Service providers

Draft CPS 230 incorporates and updates requirements for the use of service providers, with a focus on those deemed to be material. While the existing standards, CPS 231 and SPS 231, set out requirements for outsourcing (activities that the entity could undertake itself), draft CPS 230 emphasises the broader use of service providers, reflecting the increased reliance on third parties to undertake critical operations.

This shift from focusing purely on outsourcing arrangements to a more expansive range of service offerings reflects the variety of delivery models now used by regulated entities. Furthermore, the proposed standard also broadens from focusing on the outsourcing policy, upfront due diligence and service level agreements to risk management at all stages of a service provider arrangement - from initiation through to exiting the arrangement.

Material service providers

Draft CPS 230 would require an APRA-regulated entity to identify its material service providers and manage the risks associated with the use of these providers. A material service provider is one on which an entity relies on to undertake a critical operation or that could expose it to material operational risk. Draft CPS 230 includes a list of the types of services that would be classified as material (refer Table 6). There may be other service providers that an entity uses that they determine to be material to their operations.

Table 6. Services that would be material

Banking	Insurance	Superannuation
Services supporting critical operations	Services supporting critical operations	Services supporting critical operations
Risk management	Risk management	Risk management
Core technology services	Core technology services	Core technology services
Internal audit	Internal audit	Internal audit
Credit assessment	Underwriting	Fund administration
Funding and liquidity management	Claims management	Custodial services
Mortgage brokerage	Insurance brokerage	Investment management
	Reinsurance	Arrangements with promoters and financial planners

Managing risks associated with service providers

A Board-approved policy on the management of service providers is critical for managing risks associated with reliance on service providers, whether related or unrelated to the entity. An APRA regulated entity's service provider management policy would cover its approach to entering into, monitoring and exiting arrangements and, crucially, how the entity will manage the risks associated with the use of service providers.

All arrangements involving material service providers would be formalised through a binding legal agreement. Draft CPS 230 includes key criteria to be addressed as part of the legal agreement and matters that APRA considers are sufficiently material to need to be included. The legal agreements ensure that each party's obligations are clear and limits legal risk to the extent practical.



Fourth party risk management

With an increasing reliance on service providers, there is greater complexity in supply chains; a number of service providers may be involved in providing a service to an APRA-regulated entity. A regulated entity may have a direct agreement with a service provider (a third party) who, in turn, is reliant on another service provider for the provision of a service (a fourth party). In certain cases, these fourth party service providers can, in turn, be reliant upon yet another service provider. This can result in APRA-regulated entities relying on downstream service providers without a direct agreement in place, which can impede their ability to manage risks in the supply chain.

Draft CPS 230 would require a regulated entity's service provider management policy to set out its approach to managing risks with fourth parties.¹⁰ APRA expects that entities would also seek to be aware of, and manage, the risks associated with any further downstream service providers, to maintain a thorough understanding of the supply chain and potential issues that could affect the entity's ability to maintain critical operations.

Monitoring and notifications

APRA has sought to balance notification requirements and the need to provide documents or other information, to minimise the compliance impact both in terms of time and cost on regulated entities. Notification is only needed where there are matters that APRA supervisors should reasonably be made aware of, and which could have broader systemic implications.

Under draft CPS 230, an entity would be required to:

- submit its register of material service providers to APRA on an annual basis;

¹⁰ Currently, CPS 231 and SPS 231 require sub-contracting to be addressed in an outsourcing contract, with an indemnity to the effect that any sub-contracting by a third-party service provider is the responsibility of the third-party service provider.

- notify APRA as soon as possible, and not more than 20 business days, after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation; and
- notify APRA prior to entering into any offshoring agreement with a material service provider, or when there is a significant change proposed to the agreement, including in circumstances where data or personnel relevant to the service being provided will be located offshore.

Submitting the register of material service providers will enable APRA to assess the nature and extent of service providers relied on by each industry, with a view to identifying and responding to potential systemic issues. For example, concentration risk could arise where multiple entities are reliant on a single provider or a small number of providers for a particular service. While such concentration may be unavoidable, awareness of such risks will allow consideration of actions that could reasonably be taken to mitigate the risk or deal with issues should they arise.

Service providers in superannuation

The duties of RSE licensees under the *Superannuation Industry (Supervision) Act 1993* (SIS Act) and the focus on the delivery of outcomes to members makes operational risk management particularly important in superannuation.

RSE licensees have typically outsourced many material business activities to service providers, including related parties. These service providers play a crucial role in the RSE licensee's business operations. Given this, it is important that an RSE licensee board reviews risk and performance reporting on service provider arrangements and ensures that the RSE licensee continues to meet its obligations under the SIS Act.

RSE licensees' statutory duty to prioritise the interests of members, and manage actual and perceived conflicts is unique to superannuation (refer to s. 52(2)(d) of the SIS Act and *Prudential Standard SPS 521 Conflicts of Interest* (SPS 521)). Managing conflicts is particularly important with respect to service provider arrangements, with a strong onus on the board to oversee the performance of service providers to fulfil their obligations under the SIS Act. This is reflected in draft CPS 230, including a requirement for an entity to be able to terminate an agreement in a situation where it is inconsistent with the best financial interest duty.

Draft CPS 230 has also been informed by findings from the APRA-commissioned review of outsourcing arrangements of ten selected RSE licensees.¹¹ While the review observed strong compliance with SPS 231 and *Prudential Standard SPS 521 Conflicts of Interest*, and an uplift in board oversight, several areas for improvement were identified. These included the need for a genuine assessment of service providers, robust performance monitoring and functional independence to oversee service providers.

¹¹ The thematic review was undertaken in response to observations made by the Royal Commission regarding deficiencies in the management of outsourcing arrangements in superannuation, including the identification and management of conflicts of interest connected with related party outsourcing arrangements.

Chapter 5 - Consultation and next steps

Request for submissions

APRA invites written submissions on the proposals set out in this Discussion Paper and the accompanying draft CPS 230. Written submissions should be sent to PolicyDevelopment@apra.gov.au by 21 October 2022 and addressed to the General Manager, Policy, APRA.

Following review of feedback and submissions received, APRA plans to finalise the standard in early 2023 and release draft guidance for consultation. The proposed CPS 230 would come into effect from 1 January 2024.

Consultation questions

APRA welcomes feedback on the proposed requirements in CPS 230. The following questions are intended to identify specific areas for feedback that would assist APRA in finalising the requirements. They are intended to support, but not limit, responses.

Table 7. Key questions

Overall design	<ol style="list-style-type: none">1. Is a single cross-industry standard for operational risk management supported?2. Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?3. How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?4. What are the estimated compliance costs and impacts to meet the new and enhanced requirements?
Specific requirements	<ol style="list-style-type: none">5. How could APRA improve the definitions of critical operations, tolerance levels and material service providers?6. What additions or amendments should be made to the lists of specified critical operations and material service providers?7. Are the notification requirements and the time periods reasonable?8. What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?

Request for cost-benefit analysis information

APRA requests that all interested stakeholders use this consultation opportunity to provide information on the compliance impact of the proposed changes and any other substantive costs associated with the changes. Compliance costs are defined as direct costs to businesses of performing activities associated with complying with government regulation.

Specifically, information is sought on any increases or decreases to compliance costs incurred by businesses as a result of APRA's proposals.

Consistent with the Government's approach, APRA will use the methodology behind the Commonwealth Regulatory Burden Measure to assess compliance costs. This tool is designed to capture the relevant costs in a structured way, including a separate assessment of upfront costs and ongoing costs. It is available at <https://rbm.obpr.gov.au/>.

Respondents are requested to use this methodology to estimate costs to ensure the data supplied to APRA can be aggregated and used in an industry-wide assessment. When submitting their costs assessment to APRA, respondents are asked to include any assumptions made and, where relevant, any limitations inherent in their assessment.

Feedback should address the additional costs incurred as a result of complying with APRA's requirements, not activities that entities would undertake regardless of regulatory requirements in their ordinary course of business.

Important disclosure notice — publication of submissions

All information in submissions will be made available to the public on the APRA website unless a respondent expressly requests that all or part of the submission is to remain in confidence. Automatically generated confidentiality statements in emails do not suffice for this purpose. Respondents who would like part of their submission to remain in confidence should provide this information marked as confidential in a separate attachment.

Submissions may be the subject of a request for access made under the *Freedom of Information Act 1982* (FOIA). APRA will determine such requests, if any, in accordance with the provisions of the FOIA. Information in the submission about any APRA-regulated entity that is not in the public domain and that is identified as confidential will be protected by section 56 of the *Australian Prudential Regulation Authority Act 1998* and will therefore be exempt from production under the FOIA.

Attachment A: Policy options

APRA initiated consultation on updating its requirements for operational resilience in 2018, with the release of a discussion paper and draft prudential standard on information security management. As APRA noted at that time, its preferred approach was to prioritise information security given the heightened risk in that area.

Following on from this, APRA noted that it would consult on prudential requirements on the management of operational risk more broadly, including updated requirements for business continuity and outsourcing. This Discussion Paper is the second stage in that stepped process to updating the prudential framework for operational resilience.

The discussion paper in 2018 outlined three policy options for developing and updating prudential standards and guidance on operational resilience.¹² Those three options are summarised in the table below.

Table 8. Policy options

Option	Approach
Option 1: Status quo	Continue with the existing standards and guidance, relying on supervisory discretion to address any deficiencies in the risk management practices of entities.
Option 2: Stepped approach	Introduce prudential requirements on information security, ahead of other requirements on the qualitative management of operational risk.
Option 3: Simultaneous approach	Introduce a prudential standard on the qualitative management of operational risk, which includes revised content on business continuity and outsourcing, and new content on information security.

Option 1 – Status quo

Under this option, APRA-regulated entities would continue to follow existing standards and guidance, and APRA would rely on supervisory discretion to address any deficiencies in risk management practices. This may, however, lead to inconsistencies across entities and the potential for minimum expectations not being met across the industry.

Option 2 – Stepped approach

Under this option, APRA would prioritise information security management and introduce prudential requirements on information security, and then develop standards for operational risk management more broadly. This option will focus industry’s attention on the highest priority risk area; APRA considers that an information security event could have a material impact on an entity.

¹² [Information security management: a new cross-industry prudential standard](#), APRA, 7 March 2018

Option 3 – Simultaneous approach

Under this option, APRA would introduce new prudential standards on operational risk management, and information security, and revise prudential standards on business continuity and outsourcing.

APRA noted in its discussion paper in 2018 that its preferred approach was Option 2: Stepped approach. Draft CPS 230 is consistent with this approach. As noted above, APRA invites respondents, as part of their submission, to provide information on the compliance impact of draft CPS 230, and any other substantive costs associated with the proposed requirements.



APRA