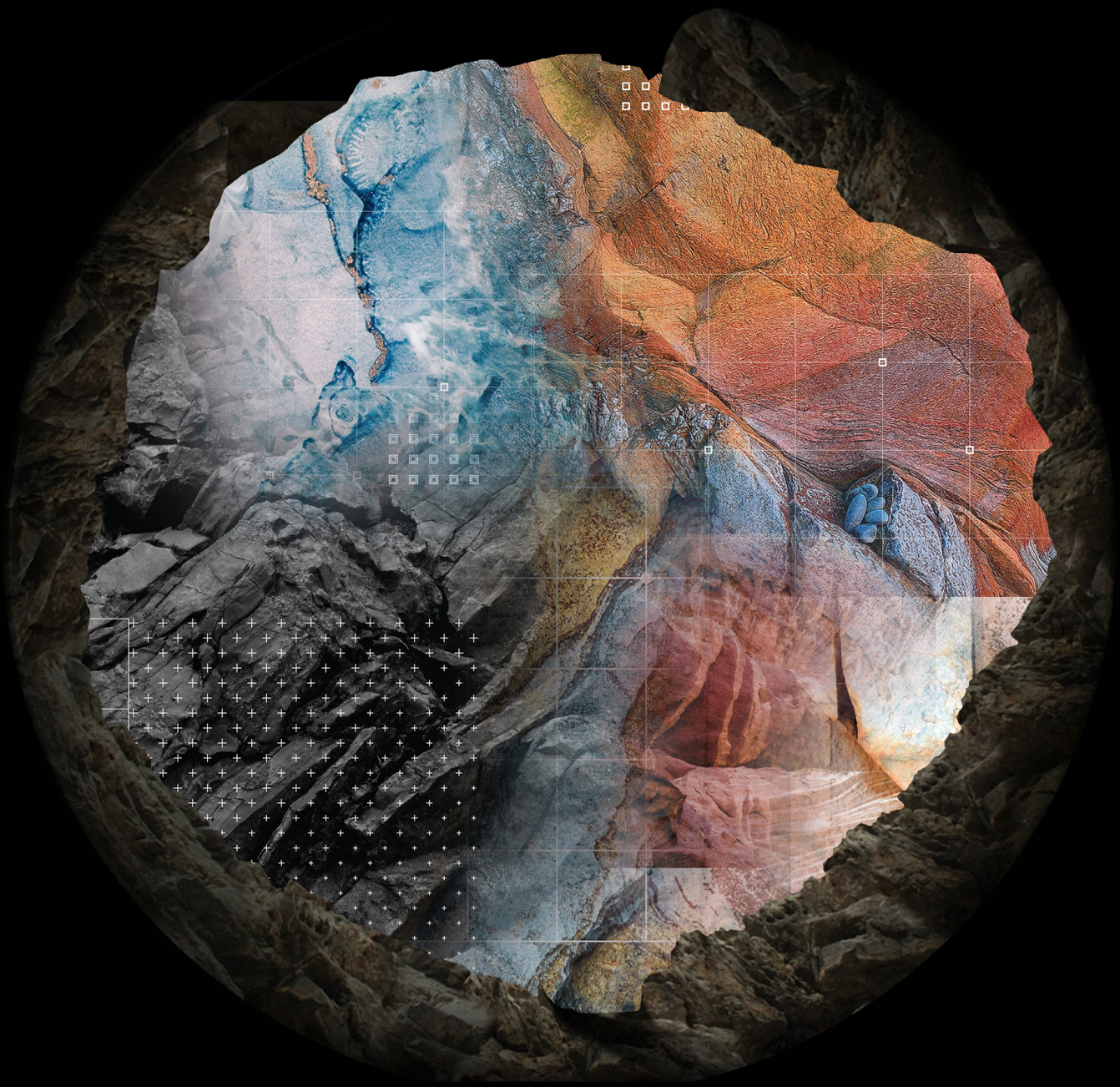
Deloitte.



CPS 230: Operational Risk Management

Strengthening the resilience of the financial services ecosystem

Table of contents

01

The importance of operational resilience has never been clearer. The industry has experienced a broad and multi-faceted range of operational risks – disruptions to supply chains, technology incidents, high-profile compliance failures, geopolitical and economic uncertainty. At the same time, COVID-19 has tested the resilience of financial services institutions beyond imaginable scenarios, and cybersecurity threats are becoming the norm.

CPS 230: Operational Risk Management | Executive Summary

Executive Summary

The pandemic has highlighted a pressing need for organisations to be more resilient and prepared to confront a spectrum of known and unknown risks. This includes 'grey swan' events – seemingly unlikely events that are nevertheless possible and severely impactful.

The concept of '*operational resilience*' isn't new. Conventional thinking, however, has limited this understanding to business continuity. Organisations now have greater clarity on what true operational resilience entails and the value it can derive, including increased adaptability and agility, better decision making and improved customer outcomes. Regulators globally have recognised its importance and are bringing it within the scope of their regulatory framework.

In our view, an operationally resilient organisation has the foresight to plan for uncertainties and can quickly adapt and absorb the impacts of a range of disruptions. It considers not only "*what-ifs*" but also "*what next*". It is rooted in robust operational risk management but requires a holistic and multi-disciplinary approach across business continuity planning, third party management, and cyber and information security. Most importantly, it is backed by proven outcomes and capabilities.

Consistent with global regulatory trends, Australian Prudential Regulatory Authority (APRA) has sharpened its focus on the operational and financial resilience of the financial services industry. This includes the recent introduction of new cross-industry prudential standards: *CPS 230 Operational Risk Management*, *CPS 900 Resolution Planning* and *CPS 190 Financial Contingency Planning*.

This paper focuses on APRA's draft *CPS 230: Operational Risk Management (CPS 230)*. CPS 230 brings into scope new and enhanced requirements with respect to operational risk management, business continuity planning and service provider management.

At its core, CPS 230 firmly places accountability for operational risk management on the Board and seeks to reduce the impact of disruptions on customers, market participants and the financial system. The standard aims to ensure critical operations are maintained through severe but plausible business disruptions, and risks associated third and fourth-party service providers are managed more effectively.

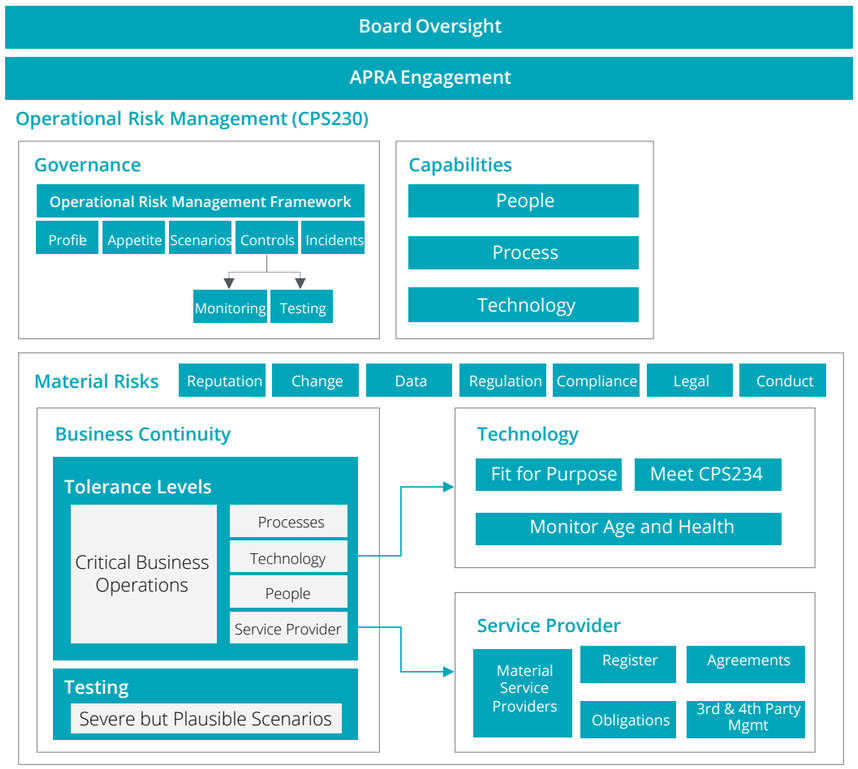
As APRA-regulated entities look to implement these regulatory changes, it is an opportune time to reconsider their operating model and operational resilience capabilities.

In this paper, we share our perspectives on the key changes and implications of the draft CPS 230, the benefits of operational resilience, and the practical steps regulated entities can take while awaiting the finalised standard.

02

CPS 230 Framework

Compliance with CPS 230 will require considered design and coordination across a number of core elements. The diagram below demonstrates the interaction between these elements.



Overview of CPS 230

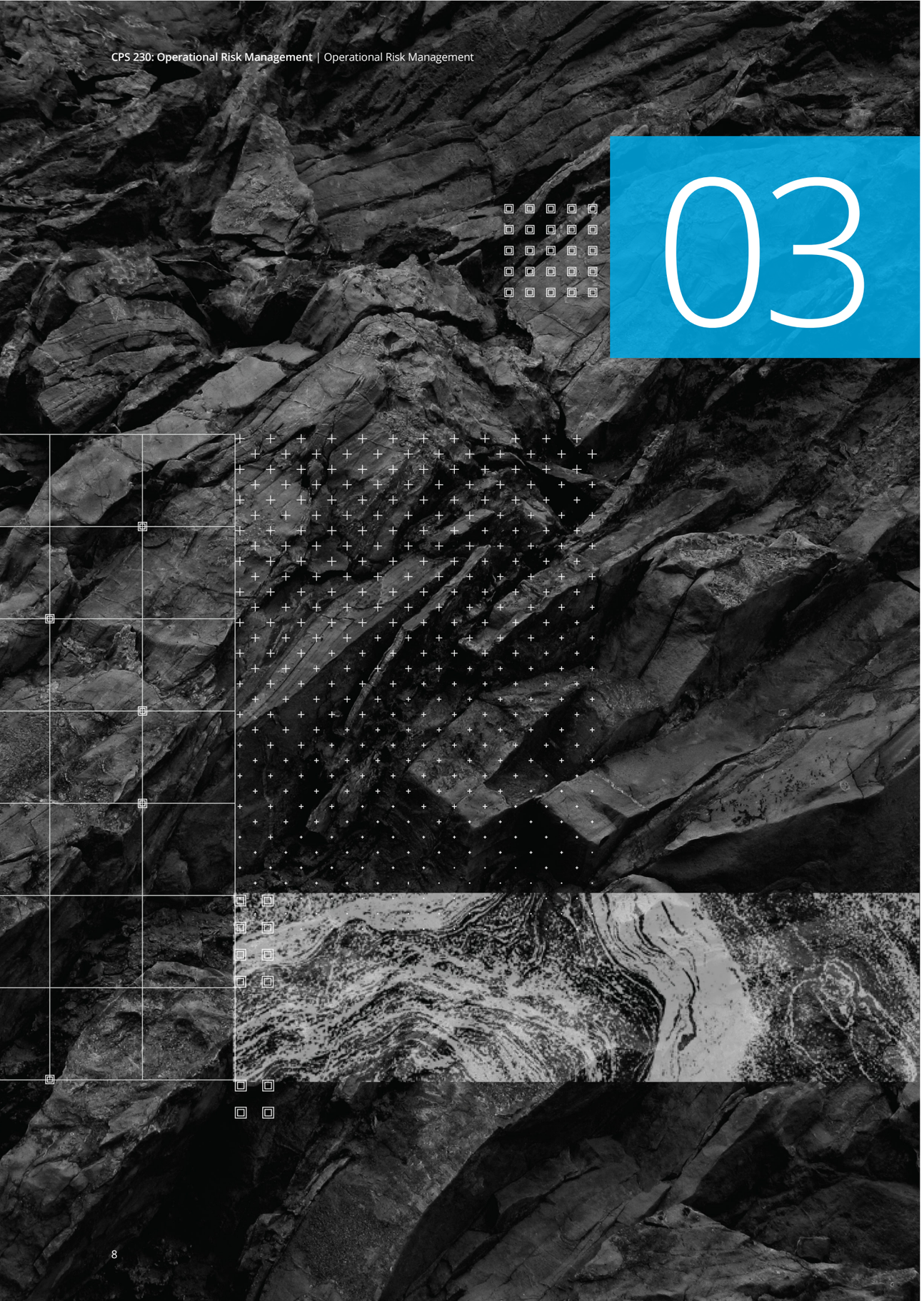
The proposed CPS 230: *Operational Risk Management* supersedes existing prudential standards1 and introduces new and enhanced requirements to better align with global standards and industry leading practices.

Key changes and implications

Summarised below are our perspectives on the key changes in CPS 230. Further details are provided in later sections.

Today	January 2024
Critical Business Operations Critical business operations are typically identified from the perspective of the entity by assessing the impact on the entity should critical business operations be unavailable.	**Critical Operations** Take an 'outside-in' view and shift the focus from what is critical to the organisation to what is critical to customers, market participants and the financial system more broadly.
Recovery Timeframes As part of conventional business continuity planning, entities have identified Maximum Allowable Outages (MAOs) (or Maximum Tolerable Periods of Disruptions (MTPD)), and Recovery Time Objectives (RTO).	**Tolerance Levels** Define not just how long a critical operation can be disrupted for, but *how much and for how long* before the impact is intolerable. In addition to setting recovery timeframes, identify Maximum Data Losses and Minimum Recovery Objectives or Service Levels.
Management of Material Outsourced Providers Existing policies are typically focused on the management of third-party service providers performing material business activities that would otherwise be performed 'in-house', with monitoring activities usually limited to a review of their performance against agreed service levels. Additionally, entities largely rely on contractual agreements with third parties to mitigate risks associated with fourth-parties.	**Management of Material Service Providers, incl. Fourth Parties** Expand the scope beyond outsourced service providers and identify material service providers (incl. third and fourth parties, partners, suppliers and affiliates) that enable critical operations or expose the organisation to material operational risks. Additionally, ensure risks presented by third and fourth parties are managed proactively and comprehensively on an ongoing basis.
Testing and Review against BCM Objectives Scenarios used for testing are often limited in scope (e.g. only testing a sub-set of critical operations) and/or based on generic unavailability scenarios that are 'contained and plausible' (e.g., unavailability of technology or an office location).	**Testing and Review Against Tolerance Levels** Establish a more robust testing and review program which includes all critical operations and material risks, and assesses the entity's ability to maintain business operations within tolerance levels through '*severe but plausible*' disruptions.
Board Responsibility Operational risk responsibilities have been steadily shifting towards Line 1 Management, there is still a heavy reliance on risk management functions to maintain end-to-end oversight, and no enforced linkage between Board and Senior Management decision making and the impact of these decisions on the resilience of critical operations.	**Board Accountability** Place *accountability*, not just *responsibility*, on the Board and senior management to oversee and manage operational risk, end-to-end. Risk reporting should be clear on the impacts to the resilience of critical operations.
Broad Focus on Material Risks Entities are only required to maintain a risk management framework which addresses material risks – broadly defined as those with a financial or non-financial 'material' impact on the institution, its depositors and/or policyholders.	**Clear Linkage to Operational Resilience** Review and update the entity's operational risk profile to ensure it comprehensively considers critical operations, approved tolerance levels and interdependencies with third and fourth parties. Risk profiling activities should also consider operational risk incidents and near misses.

[1] CPS 230 will replace Prudential Standard CPS 231 and SPS231 Outsourcing; CPS 232 and SPS232 Business Continuity Management; and Prudential Standard HPS 231 Outsourcing.



03

Operational Risk Management

The proposed standard stresses accountability and responsibility of the Board and Senior Management to actively oversee and manage operational risks.

The following section summarises key changes introduced by CPS 230 with respect to **operational risk** and provides key considerations for regulated entities as they prepare for the implementation of the standard.

3.1 Linkage to Resilience

Ensure comprehensiveness of operational risk management activities, and clear linkage to the resilience of critical operations within approved tolerance levels, rather than broadly defined 'material risks'.

Current state

- Regulated entities are presently only required to maintain a risk management framework which addresses material risks – broadly defined as those with a financial or non-financial 'material' impact on the institution, its depositors and/or policyholders.
- In most cases, there is no clear link between risk management activities and their ability to support the continuation of critical operations within approved tolerance levels across the end-to-end value chain.

Key Considerations for CPS 230

- Entities should review and update their operational risk profile to ensure it comprehensively considers critical operations, approved tolerance levels and interdependencies with third and fourth parties. Risk profiling activities should also consider operational risk incidents and near misses.
- Additionally, entities will also need to:
  - Review and if required, uplift processes to identify, report and remediate material weaknesses (taking into consideration defined critical operations and tolerance levels);
  - Ensure there is a process to comprehensively identify, assess, treat and monitor operational risk regularly, particularly where any business decisions are made, or issues and incidents arise that might impact the resilience of critical operations; and
  - Review and where necessary, improve mechanisms to monitor the age and health of IT infrastructure supporting critical operations and risk management.

3.2 Accountability and Ownership

Place accountability, not just responsibility, on the Board and senior management to oversee and manage operational risk, end-to-end. Risk reporting should be clear on the impacts to the resilience of critical operations.

Current state

- While operational risk responsibilities have been steadily shifting towards Line 1 management, in some instances, there is still a heavy reliance on risk management functions to maintain end-to-end oversight.
- Further, there is no enforced linkage between Board and senior management decision making and the impact of these decisions on the resilience of critical operations.

Key Considerations for CPS 230

- Entities should consider reviewing and updating the Board charter and roles and responsibilities for senior management to explicitly embed operational risk management considerations in decision making, particularly the impact of decisions on the resilience of critical operations.
- Entities should also update triggers for and coverage of Board reporting to ensure the impact on the resilience of operational risk on the resilience of critical operations is clear and communicated in a timely manner.

3.3 APRA Notification

Notify APRA within 72 hours after becoming aware of an operational risk incident that has a material financial impact or a material impact on a critical business operation.

Current state

- The current requirement under CPS 220 Risk Management[2] requires entities to only report any material revisions to the:
  - Risk appetite statement
  - Business plan
  - Risk management system
- Any significant breaches or material risks are required to be reported within 10 days. The current standard does not include an explicit requirement for the reporting of operational risk incidents.

Key Considerations for CPS 230

- Entities should consider data and reporting requirements for prompt detection of material operational risk incident, and uplift monitoring capability where required.
- Entities should also update APRA reporting triggers in line with the 72-hour timeframe required under the CPS 230 and where appropriate, align with existing CPS 234 Information Security incident reporting processes.

[2] CPS 230 Operational Risk Management underpins CPS 220 Risk Management.

CPS 230: Operational Risk Management | Operational Risk Management

04

Business Continuity Management

Regulated entities will need to adjust the scope of their business continuity management program and review their definition of criticality to include the perspectives of a broader stakeholder group.

The following section summarises key changes introduced by CPS 230 with respect to **business continuity** and provides key considerations for regulated entities as they prepare for the implementation of the standard.

4.1 Critical Operations

Take an 'outside-in' view and shift the focus from what is critical to the organisation to what is critical to customers, market participants and the financial system more broadly.

Current state

- Traditionally, entities have identified critical business operations by primarily assessing the impact (e.g. financial, legal, regulatory, reputational) on the entity should critical business operations be unavailable.

Key Considerations for CPS 230

- When identifying and assessing critical operations, entities should consider:
  - How products and services delivered by the organisation are being perceived and relied upon;
  - The entity's role in the financial system;
  - How it would impact customers, market participants, the financial system and any other key stakeholders if the products or services were disrupted; and
  - Key resources and dependencies (e.g. systems, data, people, premises, suppliers, vendors and partners) which underpin critical operations.

4.2 Tolerance Levels

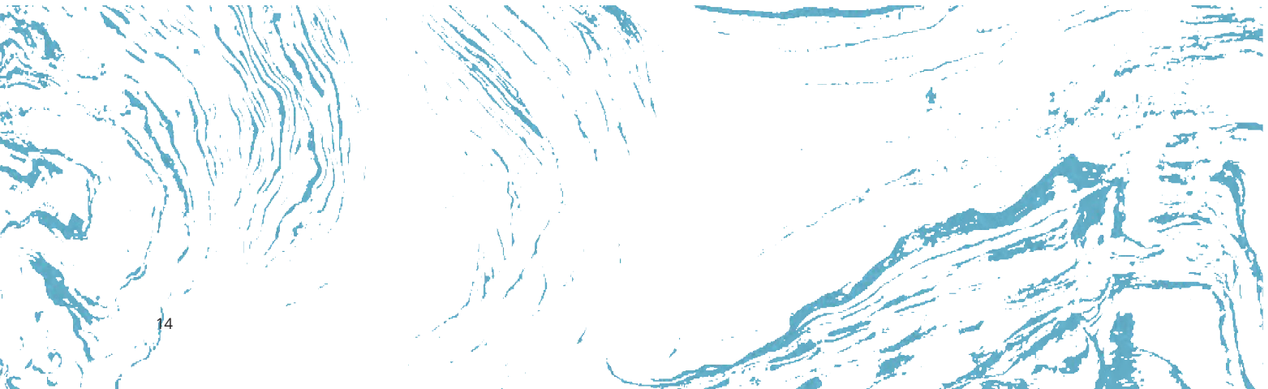
Define not just how long a critical operation can be disrupted for, but how much and for how long before the impact is intolerable.

Current state

- As part of conventional business continuity planning, entities have identified Maximum Allowable Outages (MAOs) (or Maximum Tolerable Periods of Disruptions (MTPD)), and Recovery Time Objectives (RTO).
- More mature entities will also be familiar with the concepts of Maximum Data Losses and Minimum Recovery Objectives.

Key Considerations for CPS 230

- In addition to setting recovery timeframes, entities should ensure Maximum Data Losses and Minimum Recovery Objectives or Service Levels have been consistently defined for each critical operation identified.
- Tolerance levels should be customer and outcomes focused, justifiable and Board-approved.
- When setting these tolerance levels, entities should consider:
  - Business-As-Usual' (BAU) service levels (i.e., the metrics that best describes the functioning of critical operations during BAU); and
  - The service levels needed during a disruption and by when, in order to avoid intolerable harm to customers, market participants, the financial system and other key stakeholders
- As an example, in the event of a disruption to outbound customer payments, an entity may set their tolerance level to be 30% completion rate within 4 hours.



4.3 Testing and Exercising

Establish a robust and systematic testing program to test plans and tolerance levels against severe but plausible scenarios.

Current state

- While most entities are already testing their business continuity plans annually, scenarios used for testing are often limited in scope (e.g. only testing a sub-set of critical operations) and/or based on generic unavailability scenarios that are contained and plausible (e.g., unavailability of technology or an office location).
- Additionally, tests performed are often confined to desktop exercises that do not assess an entity's ability to meet RTOs.

Key Considerations for CPS 230

- Entities should ensure the scope of the testing program includes all critical operations and material risks. The testing should not only assess plans but also tolerance levels against a range of severe and plausible disruption scenarios.
- A severe but plausible scenario would include disruptions of significant scale where recovery timeframes and service levels cannot be achieved using pre-planned recovery measures and extraordinary contingency arrangements may be needed. For instance, the failure of IT services of such scale that a failover to an alternate data centre in accordance with IT disaster recovery plans is not sufficient or feasible.

4.4 Monitoring, Review and Reporting

Implement mechanisms to monitor and report compliance with tolerance levels and provide greater assurance to the Board on the credibility of the Business Continuity Plans in maintaining critical operations within tolerance levels.

Current state

- The level of Board oversight on the effectiveness of business continuity arrangements varies significantly across entities, with responsibility for oversight often delegated to Management.
- Internal audits are also typically limited in scope and focused on ensuring plans have been developed in alignment with the Organisation's Business Continuity Policy.

Key Considerations for CPS 230

- The proposed standard by APRA places greater emphasis on the Board having the relevant information to allow it to discharge its responsibilities and make informed decisions, as well as having oversight of any failure to meet tolerance levels and plans for remediation.
- Entities should ensure that Internal Audit activities include an assessment of whether Business Continuity Plans include realistic procedures and measures describing how the organisation will maintain critical operations within tolerance levels through severe disruptions.

05

Service Provider Management

Given an increasing reliance on service providers and an increasingly complex and interconnected financial services ecosystem, regulated entities will also need to have a clearer understanding of their third and fourth parties, and ensure their associated risks are monitored and managed comprehensively.

As CPS 230 introduces new and enhanced requirements, organisations need to consider three key changes to **service provider management**:

5.1 Material Service Providers

Expand the scope beyond outsourced service providers and identify and document service providers that also enable critical operations or expose the organisation to material operational risks.

Current state

- Existing organisational policies are typically focused on the management of outsourcing arrangements and the service providers performing material business activities that would otherwise be performed 'in-house'.
- These policies do not necessarily take into account the broader ecosystem of partners, suppliers and affiliates that organisations may rely on to transform their operating model, business models or value propositions.

Key Considerations for CPS 230

- The proposed standard will require the development of a comprehensive service provider management policy and a register of material service providers. The policy should outline the organisation's approach to identifying and managing material service providers (incl. fourth parties) and their associated risks.
- As entities review their definition of materiality and identify material providers, the following should be considered:
  - The types of services APRA has identified as being material;
  - Whether the service provider supports or enables critical operations;
  - The impact on critical operations and the organisation's ability to maintain critical operations within tolerance levels in the event of a disruption impacting the service provider;
  - The scope and number of arrangements in place with a service provider;
  - Whether the service provider would be difficult to substitute; and/or
  - The level of risk associated with the service provider across risk domains (e.g. information security, legal and regulatory compliance, business continuity).

5.2 Risk Management and Monitoring

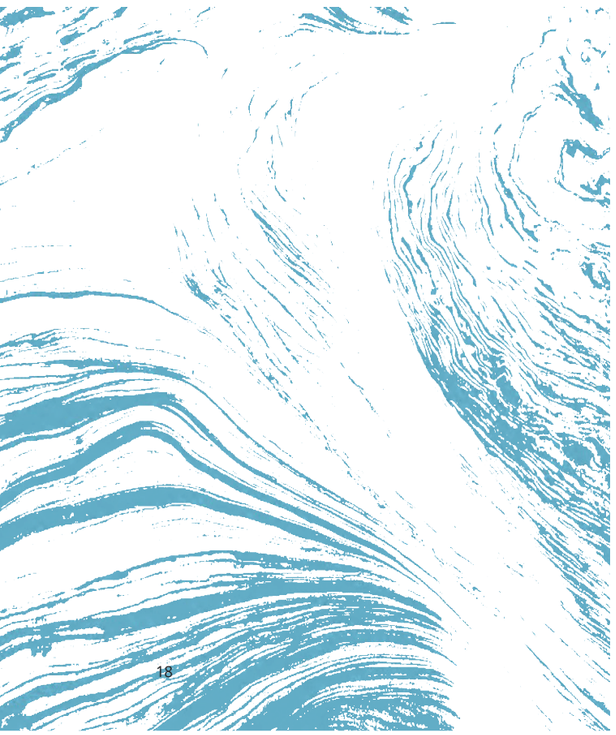
Ensure risks presented by material service providers (incl. third, related parties and connected entities) are managed comprehensively and on an ongoing basis.

Current state

- The due diligence process performed prior to selecting and onboarding a service provider is often limited to an assessment of their ability to conduct business activities on an ongoing basis.
- Monitoring activities are also often largely focused on the performance of material outsourced providers against agreed service levels.

Key Considerations for CPS 230

- The proposed standard recognises the importance of managing over-reliance on service providers and imposes more prescriptive requirements for risk management and monitoring.
- Entities will need to ensure that "*financial and non-financial risks from reliance on a particular service provider, including risks associated with geographic location or concentration of the service provider(s) or parties the service provider relies upon in providing the service*"[3] are carefully considered and managed on an ongoing basis.
- This will require an understanding of service providers who may directly or indirectly support critical operations (e.g. a service provider may directly support the organisation as well as support other service providers of the organisation, thereby presenting a heightened level of risk).
- In addition to monitoring performance against agreed service levels, entities will also need to monitor the effectiveness of their controls in managing risks associated with material service providers and compliance with the service provider agreement.



[3] Draft CPS 230 Operational Risk Management, paragraph 52(b)

CPS 230: Operational Risk Management | Service Provider Management

5.3 Fourth Parties

Have greater oversight of fourth party service providers and proactively manage their associated risks.

Current state

- In alignment with CPS 231 Outsourcing , organisations are typically reliant on their contractual agreement with third party service providers to ensure any underlying risks associated with sub-contractors or 'fourth parties' are appropriately managed.
- Entities may request information from their third parties on their approach to managing fourth parties however many do not currently have a holistic and accurate view of their fourth parties, and as such their inherent risks.

Key Considerations for CPS 230

- CPS 230 introduces requirements on entities to have awareness of, and manage, the risks associated with fourth parties.
- When identifying fourth parties, entities should consider:
  - The fourth parties that underpin or support the services provided by material third party service providers;
  - How significant these fourth parties are to material third party service providers
  - Whether the fourth parties may have access to the organisation's data or may engage directly with the organisation's customers;
  - The risks identified by material third party service providers for their fourth parties;
  - Any other fourth party may not be significant to material third party service providers but may be common across multiple service providers
- To manage the risks associated with fourth parties, entities should consider:
  - How third party service providers manage and monitor the risks associated with fourth parties;
  - Requesting access to the risk and control assessments performed by material third party service providers for fourth parties;
  - Performing an independent review of key fourth parties; and
  - Revising contract terms to enable the above and ensure third parties are required to notify the organisation prior to sub-contracting.

06

Beyond compliance with CPS 230, robust operational resilience capabilities can deliver strategic benefits

Benefits of Operational Resilience

Faster and more effective crisis response

- An overarching operational resilience framework enables a harmonised approach to crisis management whilst reducing the time and cost of response.

Increase adaptability and agility

- Preparing for a wide range of potential threats and identifying the interdependencies of critical operations makes it easier for organisations to adapt and respond to unexpected events.

Better decision making

- Harmonising senior accountability and relevant functions will facilitate more informed decision making which explicitly consider their impact on resilience
- Moving away from siloed approaches will eliminate redundancies and reduce costs

Better customer outcomes

- Greater operational resilience reduces the frequency of reputational damage from disruptions, leading to increased customer confidence and satisfaction.

Effective and efficient allocation of resources

- Developing a clear and concise understanding of the technology services, applications and resources required to streamline existing process, reduce operating costs, improve day-to-day delivery and enhance restructuring activities.

07

CPS 230: Operational Risk Management | Next Steps

Next Steps

While waiting for APRA's finalisation of CPS 230, there are practical steps regulated entities can take today with 'no regrets' to mobilise and prepare for the implementation of CPS 230.

Industry learnings from other jurisdictions who have introduced similar regulation such as the UK and EU have demonstrated the importance of planning early and not underestimating the complexity of the tasks at hand.

While regulated entities may be able to leverage existing compliance arrangements to some extent for the purposes of CPS 230, the proposed standard will likely require a shift from the way in which operational risks have previously been considered and managed.

01. Involve your Board and Executive Committee, and discuss the key implications of CPS 230	Most Boards will not be experts in operational resilience but will need to be able to challenge and gain confidence that critical operations and impact tolerance levels have been defined appropriately and can be maintained during severe but plausible disruptions.
02. Define governance and identify stakeholders (Who will design, implement, operate and maintain?)	Given the scope of CPS 230, regulated entities will require input and effort from business units across the organisation as well as central functions, to design, implement, operate and maintain operational resilience capabilities.
03. Establish a high-level roadmap and determine indicative budget requirements to support the implementation	Plan the key steps needed to enable the implementation of the proposed standard by 1 January 2024. This will allow for any key issues or challenges to be identified early on.
04. Consider regulatory requirements holistically (beyond CPS 230) and existing arrangements that may be leveraged	As regulated entities plan for implementation, other regulatory changes should be considered (e.g., CPS 900 Resolution Planning and CPS 190 Financial Contingency Planning), including potential synergies and efficiencies that may be achieved by implementing these requirements holistically. For instance, CPS 230 and CPS 900 introduce similar concepts with respect to the identification of 'Critical Operations' and 'Critical Functions' that could potentially leverage similar arrangements.
05. Define key terms and develop taxonomies	CPS 230 is underpinned by the concept of 'Critical Operations'. Regulated entities should define the attributes of 'Critical Operations' in a way that is clearly delineated with the definition of 'Critical Function' for the purposes of CPS 900). It will also require an operations taxonomy from which critical operations can be identified.
06. Develop a methodology for the identification and assessment of Critical Operations	A robust methodology and criteria will be needed to identify and assess which operations are critical and non-critical.

Key Contacts & Authors

Caroline Brell
Financial Services Resilience Leader
cbrell@deloitte.com.au

Sean Moore
Risk Advisory Financial Services Industry Leader
semoore@deloitte.com.au

Ally MacLeod
Partner, Digital & Technology Risk
amacleod@deloitte.com.au

Erik Kronborg
Partner, Digital & Technology Risk
ekronborg@deloitte.com.au

Tommy Viljoen
Partner, Cyber Risk
tfviljoen@deloitte.com.au

Kreeban Govender
Director, Financial Industry Risk & Regulatory Services
kregovender@deloitte.com.au

Kerri Hie
Director, Financial Industry Risk & Regulatory Services, and Report Author
khie@deloitte.com.au

Tarah Unn
Senior Manager, Financial Industry Risk & Regulatory Services, and Report Author
tunn@deloitte.com.au

Cindy Nguyen
Manager, Financial Industry Risk & Regulatory Service, and Report Author
cindynguyen@deloitte.com.au

Deloitte.

Designed by CoRe Creative Services. RITM1235045