www.pwc.com.au

Navigating CPS 230

Considerations for implementing the CPS 230 Standard

June 2024

pwc

Navigating CPS 230

Sharing local insights and leveraging global experience

The fact that risks are now more interconnected, complex and dynamic means that organisations require various approaches to identify and connect risk silos. An end-to-end view of operational risk and resilience will help your organisation become more proactive in preparing for, and responding to, disruption.

We have worked alongside a number of Banking, Insurance and Superannuation organisations, as well as material service providers, since the release of APRA's CPS 230 Operational Risk Management Prudential Standard. In our conversations, these organisations sought clarification on several recurring themes.

In this paper, we explain how to tackle these common themes, informed by our local and global operational risk and resilience experience.

Common themes

- Board engagement
- Operational risk management
- Critical operations
- Tolerance setting
- Service provider management
- Service provider assurance
- People
- Technology

Board engagement

Under CPS 230, engagement of the Board (and others charged with governance, such as the senior officer outside of Australia for foreign ADI's and insurers) has so far been mainly educative, with a clear focus on Board responsibilities and accountabilities.

Where organisations have shared indicative tolerance levels with their Boards, this has typically been done for noting and discussion, highlighting that these remain a work in progress.

We anticipate that most organisations will use their existing governance groups to develop operational risk and resilience reporting, to meet the requirements of CPS 230.

Key takeaways

Bring the Board along the journey from the start.
This is a significant change, so it's important to educate them on the impact to the organisation as well as the changes to their responsibilities and accountabilities.
This can be achieved through deep-dive sessions with the Board or Board committee/s to walk-through critical operations, service provider management or specific operational risk management considerations.

Consider the design of reporting to satisfy governance and oversight requirements.
This helps ensure that end-to-end resilience remains the primary focus when data is captured during implementation work around critical operations and tolerances, service provider management, and operational risk.

The following are some questions for Boards to consider when discussing with management:

- How resilient are our critical operations?
- What is the status of our work around mapping, setting tolerances for disruption, and identifying resilience gaps?
- Where are we not capable to meet our tolerances and what are the risks?
- How does our resilience compare to our risk appetite?
- Are we comfortable accepting the identified risks or do we need to implement remediation plans?
- What work is underway to address our resilience gaps and vulnerabilities?
- How is resilience being embedded into the first line?
- In what direction are our resilience indicators trending?
- What information and reporting will we receive to be able to discharge our duties?

Operational risk management

Operational risk is broadly defined by APRA and includes significant risks such as compliance, technology and regulatory risks. Some organisations have two separate teams – one focused on the oversight of operational risks, the other focused on compliance. CPS 230 will require greater connectivity and integration across these functions.

While operational risks have been identified and are typically reported on through a functional lens, CPS 230 requires those risks to be mapped across critical operations. In some cases, a critical operation will span across functions and therefore the controls that are required to manage those risks may also need to evolve. The same principle applies to compliance obligations, technology risks, and fraud and scam risks being mapped across critical operations. As part of the implementation, it is vital that these control gaps/weaknesses are identified – and action is taken to address these.

Incident management is another crucial area that organisations are working through. This is complicated by the inevitable increase in material service providers and how incidents that occur in third, fourth/nth parties will need to be considered. The volume of incidents is likely to grow, along with the variety of sources from which these are identified (as a number may stem from service providers). Currently, organisations are clarifying the various ways in which they can identify incidents (e.g. once service providers of critical operations are identified). They are also clarifying how they will bring incident information together to inform their incident management processes. This includes agreeing the format, timeframes and information required from service providers in relation to an incident and determining its impact and reportability.

Key takeaways

For consistency and efficiency, map your operational risks and compliance obligations to critical operations as you review the organisation in parallel to assessing operational resilience.

Take the time to identify and document the key controls and identify where uplift may be required.

Prepare your incident management processes to handle greater volumes and, therefore, ensure the end-to-end process is as efficient as possible.

Critical operations

By now, many organisations have developed their critical operations identification criteria, identified the initial set of critical operations considered in scope for CPS 230, and embarked on documenting (or refreshing) their end-to-end critical operations and processes.

A common question is: ‘How deep should we be mapping our processes?’

In short: your processes need to be mapped to a level where you can confidently say that you understand the end-to-end critical operation - and more importantly - you can identify the resilience of the resources (e.g. people, technology, information, facilities and service providers) across these processes. While a granular level of detail is ideal, a degree of pragmatism is required too. Ultimately, the depth of your mapping will come down to a trade-off between the ongoing cost/time/resources required to complete and maintain this.

Key takeaways

Don’t let perfection of process maps get in the way of assessing potential resilience gaps. The value of the operational risk management program is not the maps themselves, but the ability to identify resources as quickly as possible to pinpoint operational risk and resilience dependencies and potential gaps.

Have a focussed group of stakeholders involved. Participants may include colleagues across the business, including those with expertise in the business, risk, business continuity, operations, technology and service provider management. This provides input from a range of perspectives during the exercise.

Timebox the exercise. Organisations could easily spend months mapping processes if allowed. Instead, we recommend setting yourself a ‘three to four week sprint’ to map the requirements as well as identify the tolerances. After this timeframe, there are diminishing returns and momentum can be lost.

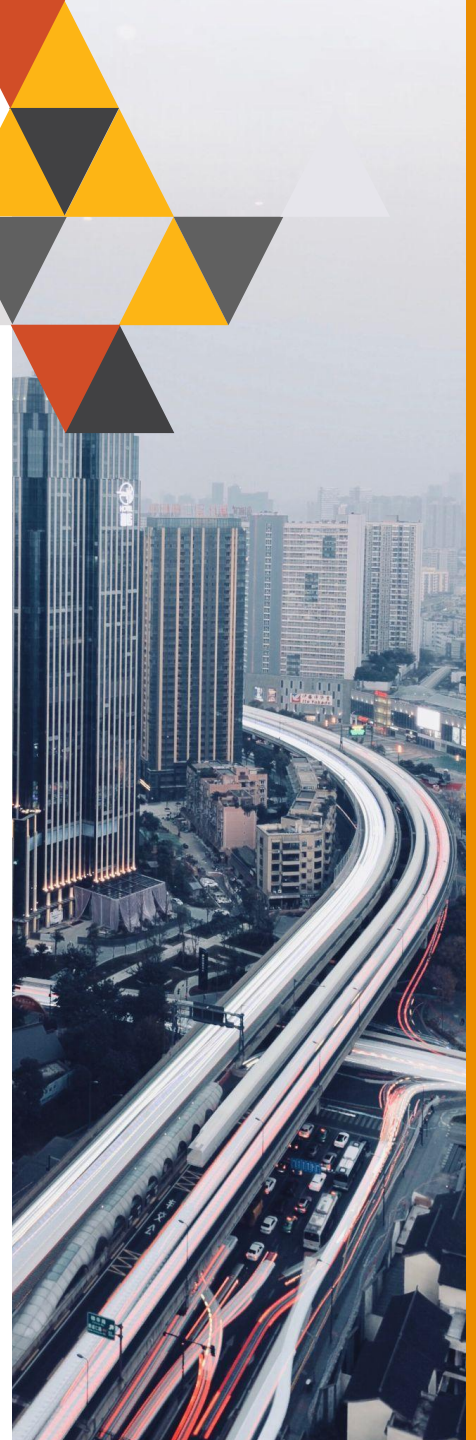
Tolerance setting

While it can be helpful to refer to the overseas approaches to tolerance setting, Australia's regime is slightly different. APRA has been relatively prescriptive, establishing three tolerance levels to capture information about: **time**, **data**, and **minimum service levels**.

Key takeaways

Tolerance levels are never perfect the first time around. It will be important to set tolerances and then utilise scenario testing to calibrate.

When a tolerance is first set, it should be considered a planning tool. Organisations should use this to understand the delta between the tolerance and factors like technology disaster recovery capability and supplier service levels.



Scenario testing

Scenario testing helps assess whether your tolerance levels were on track. It's important to define 'severe but plausible scenarios' and use these as a risk management tool to identify resilience gaps where an organisation may exceed its tolerances for disruption.

While most organisations will test scenarios relating to a 'loss of' something (e.g. technology, service provider), you should also consider scenarios where there are 'spikes in' activity (e.g. volumes of customers due to a significant disruption of a competitor).

Key takeaways

Lean on your existing scenario development and testing processes – whether they are programs for operational risk, cyber, business continuity etc or they are bespoke approaches to resilience.

Your business continuity testing should shift from 'organisation-wide' loss of facilities or technologies to how scenarios will impact critical operation(s) and how recovery would align to tolerance levels.

Consider the different types of testing to be conducted (from workshops and tabletop exercises, to simulations and data-driven approaches using operational resilience technologies).

Service provider management

Organisations should now be identifying their material service providers (MSPs) as part of the end-to-end mapping exercise of their critical operations, or those providers that can give rise to a material operational risk. It is important that all risks posed by a service provider (and their downstream providers, or '4th/nth parties') are considered.

As CPS 230 expands the scope of service provider management, the number of service providers that need to be monitored will inevitably increase. This, in turn, will require more resources to conduct criticality assessments as well as monitoring and reporting across those providers.

Many organisations are reviewing and updating their service provider management frameworks (including updates to risk assessments), identifying changes to their MSPs and any potential updates required to contracts, as well as determining the strategy and approach to update these contracts.

While organisations have until the earlier of contract renewal or July 2026 to update any existing contracts, organisations should be working with legal teams now to understand the potential uplifts to contractual clauses as these will need to be applied to any new contracts being entered into.

In terms of service provider monitoring, regulated entities will need to gain comfort over a number of aspects for MSPs, including the following:

- Governance and risk mitigation to achieve service obligations
- Programs of internal control self-assessment and testing
- Controls to govern handling of incidents and near misses
- Plans and controls for operating in the event of a severe but plausible disruption
- Incident and breach notification processes and controls (including timeliness of notification)
- Monitoring and oversight mechanisms for service providers (comprising fourth and nth parties to the APRA-regulated entities)

Key takeaways

Determine the key updates needed to service provider contractual clauses and commence early communication to relevant MSPs to allow for a smoother renewal/negotiation process.

It is likely that a number of MSPs identified for CPS 230 will have been identified for other regulatory requirements. Leverage common governance and assessment processes and uplift these, where possible.

Ensure key "4th/nth" parties are identified and the operational resilience impact of their operations to your organisation is understood.

Reporting against agreed KPIs and SLAs are a key ongoing mechanism to govern and monitor the performance of your MSPs.

Service provider assurance

Service providers are seeking to provide greater levels of assurance to their APRA-regulated entities in various ways, including:

- Allowing reviews or audits to be conducted periodically by the APRA-regulated entities
- Providing access to their own reviews of control effectiveness (including internal audit reports or external reviews)
- Working collaboratively with APRA-regulated entities to conduct scenario testing and assess operational resilience (e.g. participating in an APRA-regulated entities scenario testing)
- When testing their business continuity plans and scenario testing, consulting with the relevant APRA-regulated entity on the outcomes to allow for effective oversight and interrogation of the results

We have also seen a recent push in overseas jurisdictions to set a framework for assurance reporting over resilience controls, along with industry-wide scenario modelling. While there is no defined framework in Australia, there are benefits in having 'strength in numbers' and a consistent approach for APRA-regulated entities managing multiple service providers. Establishing a set of control objectives across groups of similar providers will ensure consistency in the market and set assurance expectations for regulated entities.

There are a range of assurance standards and reporting models available in Australia which service providers can use to enhance transparency to their regulated customers around CPS 230. While each regulated entity will inevitably define critical operations and tolerance settings according to its own unique circumstances, such assurance reporting can meet the common needs of a broad range of customers.

Key takeaways

Industry bodies who support APRA-regulated institutions are well positioned to assist with identifying common industry service providers and approaches to engagement and common assurance.

Repetitive requests and questions from APRA-regulated entities can be minimised through proactive engagement by common industry providers. This can help APRA-regulated entities to identify the necessary controls and assurance to cover the additional requirements of the Standard.

Under the new Standard, it is unlikely that a service provider's management attestations alone will be sufficient to demonstrate appropriate oversight and assurance of compliance and controls.

Where possible, entities should integrate CPS 230 requirements with other regulatory requirements (both existing and emerging) when reviewing service provider agreements and developing their oversight and assurance frameworks.

People

One of the biggest operating model challenges is shifting the management and ownership of risk, business continuity and service provider management from ‘central teams’ to the wider business. Ultimately, operational risk and resilience should be owned by the business - supported by these central teams. While accountability rests with the Board, the executive leadership team plays a key role in ensuring they demonstrate accountability for their critical operations and its resilience.

As part of the implementation of the Financial Accountability Regime (FAR), there is an opportunity to review accountability statements and accountability maps to ensure that they are correct and accurate. If, through the CPS 230 implementation, the roles and responsibilities of senior management have evolved or become more clarified as critical operations are identified, that should be reflected in accountability statements. This can be a highly effective way to reinforce accountability in the business.

Key takeaways

Ownership of operational risk and resilience should ultimately sit with your business (line 1). While the program can be led by risk functions, proactive organisations ensure the broader business takes responsibility for this too. There is still an important role for central teams to drive frameworks, consistency and alignment across business lines.

It is crucial the ‘business-as-usual’ team have clear roles and responsibilities, including their involvement and ownership during the program. Involve them early and build this into their job descriptions. This is important as resilience is not a program that finishes - it is continuous and ongoing.

Alignment is essential between your CPS 230 and FAR programs. When considering your accountability requirements under FAR, it is vital to assess how these may apply to your CPS 230 program. Forward-looking executives are taking accountability for driving the end-to-end resilience of critical operations. Organisations should take steps to review existing accountability statements in light of critical operations and their respective ownership to ensure these accurately reflect accountabilities. As part of this, you may identify that ‘accountable persons’ may require new or varied reporting or other oversight mechanisms to effectively discharge their accountabilities.

Consider the organisational change required to embed resilience into culture. Key governance and operational processes will also need to be updated to drive a ‘resilience by design’ approach across the organisation, e.g. program governance, procurement and performance measurement.

Technology

Most organisations are considering the need for technology to support the implementation of CPS 230. For operational risk and resilience programs, there is a need for a technology solution to help manage processes, dependencies, tolerance levels, scenario analyses. A technology solution can also help connect critical operations with risks, key indicators, obligations and controls. Further, an integrated tool can greatly support the identification, maintenance and management of resilience data in a ‘single source of truth’. This is far more sustainable in the longer term as an organisation’s critical operations and service providers change over time.

Key takeaways

Think strategically as well as tactically. Organisations that have not yet invested in governance, risk, and compliance (GRC) tooling are likely to take a more tactical, manual approach to data capture until they secure a business case to implement a tool(s). But even if they’re not implementing a tool immediately, most are considering a tool at least in the medium term.

Integration is vital. Most organisations already have some GRC or service provider management tool. Leverage what you have but, in doing so, assess your tool’s capability to integrate so that you can maximise the value for resilience programs. Overseas, there has been broad adoption of operational risk tooling to connect the various data sets (and existing GRC tools) into an operational resilience lens.

The better tools provide real time alerts against tolerance levels, and data driven automated scenario testing.

Key reference data sources to orchestrate resilience across a critical operation include your IT asset register/CMDB, third party register, process model and hierarchy, organisation hierarchy, data flows and metadata management. Often, these data sources require uplift and increased ongoing ownership and control to support resilience in operation.

Key actions to consider

Ultimately, operational risk and resilience can create a stronger organisation. Organisations that embed operational risk into their disciplines, processes and controls are better positioned to support their customers and stakeholders, regardless of the disruption scenarios they face.

By building their resilience and limiting the potential impact of risks, organisations are also better able to differentiate themselves when incidents occur among competitors.

With CPS 230 implementation activities well underway, at this point in time, organisations should consider the following key activities.

CPS 230 key milestones

15 July 2024
- All critical operations identified
- All material service providers identified

31 December 2024
Set tolerance for all identified critical operations

1 July 2025
Compliance with CPS 230 requirements will commence

1 July 2026
End of transition period for service provider arrangements (i.e. CPS 230 requirements relating to service provider arrangements will be in force)

Take stock

Take time to reflect on progress to date and the outlook to achieving upcoming milestones and compliance on Day 1. Key considerations include:

- What areas may have not progressed as much and are challenging? Can these be prioritised and accelerated?
- Refresh implementation activities - are they all still relevant? new activities may be coming to light that are needed and some initial actions may no longer be necessary
- Conduct a ‘lessons learned’/retrospective session off the back of pilots conducted to date and identify key learnings to inform updates to your approach

Day 1 readiness

Reflect on what Day 1 will look like and what should be in place by then. This will require considering the following:

- What capabilities and capacity will you need for compliance with CPS 230?
- What monitoring activities and new controls will need to be in place? Who will own these and perform these?
- What new reporting will be in place? And to which governance committees?
- What assurance/review will take place to check compliance against CPS 230 requirements?

These considerations may highlight additional activities that need to be undertaken and which should be incorporated within the CPS 230 implementation plan.

Optimise implementation

Consider how existing programs of work that are already underway can intersect with CPS 230 implementation to ensure alignment (e.g. FAR and other regulatory initiatives, technology transformation and product simplification) and optimise implementation effort.

In addition, where operational risk and resilience gaps are identified consider how the remedial actions and/or required investment can be integrated with other transformational programs underway.

Change management

Successful implementation of CPS 230 will be more than new processes, controls and policies. It will be about a change in culture and mindset. To do this, you should consider including organisational change management in your program.

If you haven’t already, take the time to develop a change management plan which engages the three lines of defence across the requirements of CPS 230 and what compliance will look like Day 1.

Where key sign-offs and approvals are required (e.g. by Accountable Persons, Board etc), ensure that you have engaged early and provided all the required information to enable review and oversight and approval to occur.

Contacts

Please contact any of PwC's CPS 230 team below should you wish to obtain further information.

Peter Malan
Partner, PwC Australia
Tel: +61 413 745 343
Email: peter.malan@au.pwc.com

Susanna Chan
Partner, PwC Australia
Tel: +61 414 544 066
Email: susanna.chan@au.pwc.com

Sam Hinchliffe
Partner, PwC Australia
Tel: +61 434 182 665
Email: sam.hinchliffe@au.pwc.com

Noel Williams
Partner, PwC Australia
Tel: +61 416 661 332
Email: noel.williams@au.pwc.com

Carley Bryce
Partner, PwC Australia
Tel: +61 412 929 373
Email: carley.bryce@au.pwc.com

Sara Afaghi
Partner, PwC Australia
Tel: +61 433 760 969
Email: sara.afaghi@au.pwc.com

Daniel Harb
Partner, PwC Australia
Tel: +61 433 099 889
Email: daniel.harb@au.pwc.com

Joanna Del Vecchio
Director, PwC Australia
Tel: +61 423 616 833
Email: joanna.del.vecchio@au.pwc.com

Natasha Kan
Senior Manager, PwC Australia
Tel: +61 466 050 051
Email: natasha.kan@au.pwc.com

PWC200917728