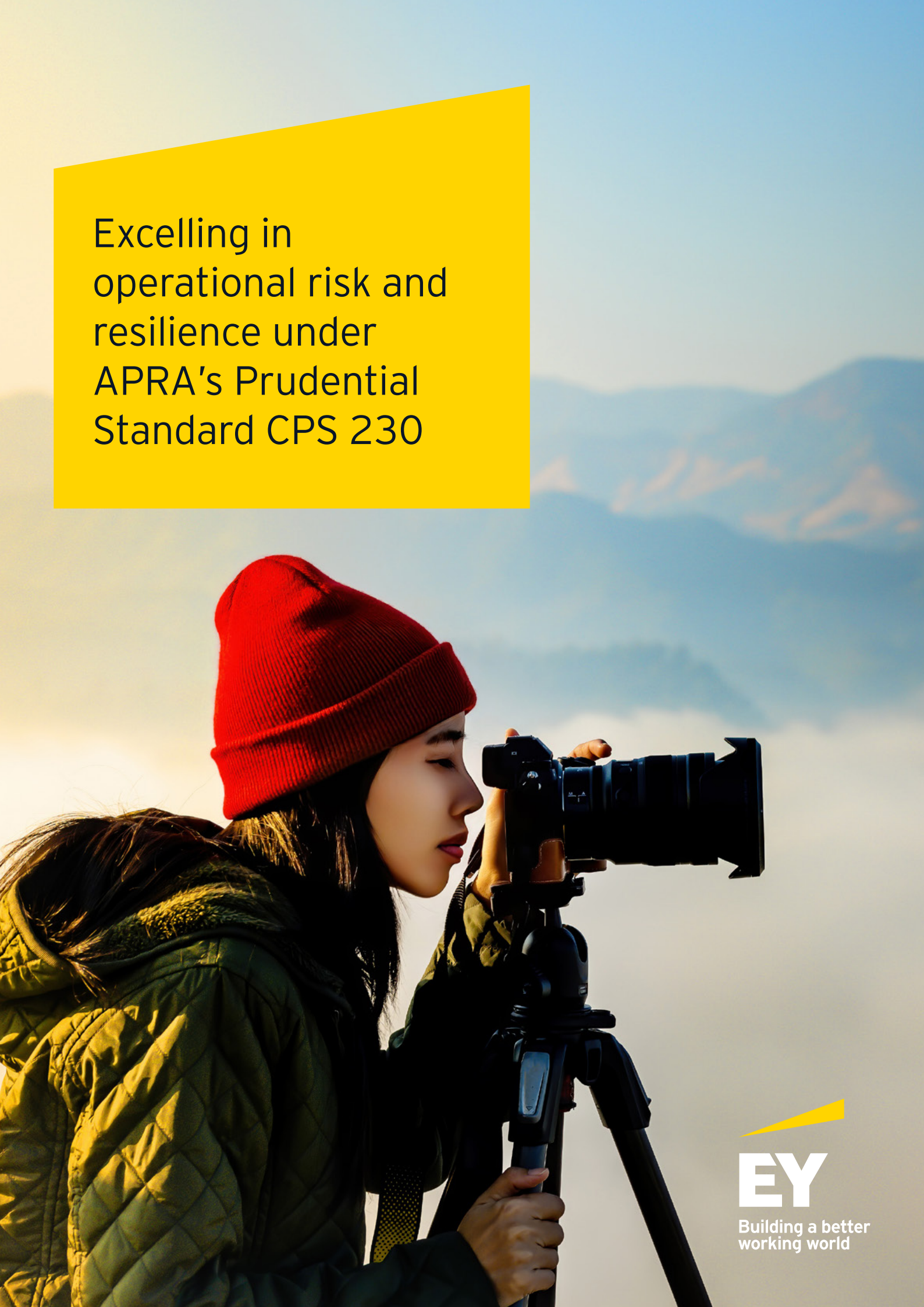
Excelling in operational risk and resilience under APRA's Prudential Standard CPS 230



Building a better working world

Contents

Introduction

The final shape of APRA's CPS 230 cross-industry operational risk management framework indicates APRA's resolute commitment to more stringent regulation of operational risk, resilience and third-party risk management practices. Although APRA's industry consultation process did change some components, the overall requirements remain virtually unchanged, with APRA proceeding in line with other world-wide regulators.

The experiences of entities in the UK and Canada suggest the compliance journey will be a time consuming, corporate-wide undertaking, touching many areas of operations. The deadline for compliance with APRA's CPS 230 has been deferred to 1 July 2025, offering some relief and more time for third-party contract renegotiations. However, entities would be ill-advised to delay compliance initiatives, which should be well underway. This is echoed by APRA's chair John Lonsdale emphasising that entities need "to be proactive in preparing for implementation, rather than waiting until the last minute to get ready to meet new requirements".

It will take at least 18 months to complete a coordinated compliance program. This paper looks at what needs to be done and offers learnings from other jurisdictions as to the likely factors for success.

What will be required to achieve full compliance by 1 July 2025?

The aim of CPS 230 is "to ensure that an APRA-regulated entity is resilient to operational risks and disruptions". In particular, it introduces first-time requirements for operational risk management, sets exacting expectations to manage APRA-defined critical operations within tolerance levels and requires more comprehensive risk management for material service providers.

As a principles-based regulator, APRA gives entities flexibility to determine their own decision-making process. However, it also signposts the need for specific board accountability. As the ultimate accountable party, the board must oversee operational risk management, approve business continuity arrangements and review the risks associated with material service providers. Boards are not the only party in the limelight. Executive management must own and manage their operational risk in the first line of defence — and not leave this to second line risk management teams.

APRA-regulated entities will need to reorganise beyond business siloes and collaborate across industry to meet the new standard. Resilience is now a 'team sport', requiring coordination and cooperation across multiple existing capabilities. Suitably competent and highly skilled teams using a common language or taxonomy, must be supported by well-integrated risk and operational teams. Specifically, entities will have to:

- **Reassess and improve operational risk management** — The standard represents a timely but challenging raising-of-the-bar, with far more prescriptive expectations for how entities need to manage their non-financial risk exposures. This will necessitate an uplift in governance and accountability. Entities must be able to identify, mitigate, and report on all the non-financial sub-risk types within an agreed appetite. Broad operational risk management processes have typically been established on the back of existing regulatory standards such as Risk Management Standard CPS 220. However, these processes have not consistently delivered risk outcomes within board-approved risk appetites, as evidenced by well-publicised failures identified in Royal Commissions. Given the more detailed requirements under CPS 230, entities should reassess and improve core principles of operational risk management. Areas for review include the relevance and currency of risk profiles, effectiveness

in operating and monitoring of internal controls, and comprehensiveness of management and board reporting.

- **Develop and integrate end-to-end critical operations processes** — The standard requires entities to take an end-to-end approach to business process mapping, covering the crucial path to deliver critical operations with a clear focus on customer outcomes. Such critical operations are rarely contained within the vertical of a function or a business silo. Instead, entities need a horizontal view of their critical operations so they can map the key components that underpin end-to-end processes. This is a very different principle to the functional organisation of most entities, likely requiring development of new processes, tools and software, and the integration of existing divisional governance structures.
- **Uplift and renegotiation of material service provider arrangements** — Regulators around the world have become increasingly concerned about the robustness of the eco-system of material service providers to the financial services industry. Locally, the results of APRA's industry-wide CPS 234 Cyber Security assessments suggest that many entities don't sufficiently understand the cyber security control environment of (non-APRA regulated) material services providers. In its own right, this raises questions about an entity's cyber resilience as a component of broader operational resilience. Under CPS 230, APRA's expanded definition of material service providers will likely lead to the identification of additional third and fourth parties, requiring entities to significantly uplift their risk management practices covering these agreements. This will include renegotiating contractual clauses to enable regular performance and risk monitoring and APRA's right to conduct on-site visits.

  As part of the compliance journey, entities can benefit from the experience and lessons learned from other jurisdictions, as well as the recently published draft CPG 230 guidance.

What are some of the critical success factors on the journey to compliance?

While the requirements of CPS 230 apply to entities, the detailed compliance journey will be dependent on a variety of factors such as size, complexity, organisational structure, and level of maturity of existing operational risk management processes. Regardless, all entities are advised to:

Keep up the momentum in compliance projects

Despite an extended timeframe for full compliance, CPS 230 will represent a significant undertaking for most entities. Compliance initiatives should be well underway, with a dedicated project team, a clear roadmap and buy-in from management and the board. The project team will need to establish a centralised approach to maintaining consistency in mapping business processes, setting tolerance levels and establishing new requirements for material services providers.

Conduct a gap analysis to direct implementation

Conducting a gap analysis will help entities to identify where policies, procedures, controls and supporting processes require uplift as well as identifying what existing practices can be leveraged. A risk appetite lens should be used to inform Day 1 minimum compliance and priority areas for uplift. This should include early and ongoing engagement with the regulator and the organisation's own board, which must approve responsibilities for uplifting the core elements of the organisation's non-financial risk framework, from reporting through to data structures. Entities with the strongest foundations will develop the most sustainable solutions to this challenge.

Include sufficient detail when mapping critical operations

In the UK, when mapping critical operations, some regulated entities did not go into enough detail and were obligated to conduct a more comprehensive analysis.

To be meaningful, critical operations mapping should include underlying business processes and their attendant people, processes, technology, data, third parties and facilities components. Entities will be able to use this information to identify and remediate vulnerabilities in achieving tolerance levels. Key criteria to determine critical operations may include the:

- Nature and size of the customer base
- Time criticality for receiving the service
- Substitutability of the service
- Potential for regulatory breach
- Impact on the entity itself, where this could cause consumer or market integrity harm
- Impact on the financial system

Set realistic tolerance levels

Entities must set tolerance levels for outage times, potential data loss and minimum service levels, within which they commit to deliver critical operations during severe disruptions to minimise material impacts on customers. Many institutions will discover their ability to meet these levels are hampered by legacy systems, manual operations and dependency on material service providers. Entities often run into difficulties when it comes to integrating the concept of impact tolerance levels with existing practices of measuring and monitoring risks. While it is important to continue to identify, measure, manage and prevent operational risk crystalising, achieving operational resilience requires entities to assume that disruptions will occur. This will require entities to perform scenario testing to confirm their ability to stay within impact tolerance levels in severe but plausible disruption scenarios. Comprehensive scenario testing should demonstrate where entities are unable to remain within impact tolerances and the steps needed to remediate these vulnerabilities. Assuming failures provides a new dimension to traditional risk management activities, including the need to cut across silos and focus on end-to-end critical operations, rather than on individual teams or IT systems.

Test controls based on the "show, don't tell" rule

One of the bigger compliance tasks will be developing an enterprise-wide controls testing and rectification program, and using it to drive continuous improvement. The standard prioritises controls based on materiality of the risks they manage, which may not even sit in a critical process. Control effectiveness must be independently assessed by an internal party who does not use the control. This is a "show, don't tell" rule, requiring proof of testing rigour. We expect to see entities using "severe but plausible" disruptive scenario analysis to test controls and identify vulnerabilities, demonstrating their ability to stay within tolerance levels.

Allow for sufficient time to renegotiate contracts with material service providers

In response to APRA-regulated entities placing greater reliance on third parties to operate critical processes, CPS 230 contains much more stringent third-party risk management requirements. If reliant on a material third-party, entities will need to:

a. Obtain assurance over the quality and accuracy of the third-party's testing approach scenarios
b. Reassess and test governance and oversight models
c. Conduct due diligence focusing on robust risk assessments, scenario tests and reporting needs
d. Update exit plans to include unplanned exit scenarios

The standard will also trigger reviews of all material service provider contracts and negotiations to revise them with new clauses, including APRA's right to conduct on-site visits and the implementation of continual performance monitoring. The moment one aspect of a contract is changed, others are likely to be brought into question. CPS 230 will not precipitate "minor updates" but full-blown renegotiations. Some suppliers may choose to exit the relationship, which will be messy. Entities will need to double down on their understanding of third and fourth party arrangements, and potentially make different choices around sourcing their external services.

Support processes with excellent data quality

The standard will raise the reporting bar on many levels, including data quality. Entities will need to ensure all risk reporting is based on robust, quality data in line with APRA's guidance on managing data risk in CPG 235. The data that larger firms already capture in their Governance Risk and Compliance (GRC) tools can be used to help proactively anticipate and manage risk and uplift the control environment. Risk profiles should be updated in a timely manner, enabled by the interconnected elements of data in the GRC tools and supported by data classification taxonomies that enable linkages to provide insights and analysis.

With the final release of the standard, APRA intends to ensure entities are well positioned to meet the challenges of a rapidly changing industry and technology landscape. As part of the compliance journey, entities will benefit from the experience and lessons learned from other jurisdictions. This should avoid a fragmented, divisional approach. By focusing on building sustainable solutions embedded in day-to-day operations, the compliance initiatives underway this year should yield measurable benefits.

EY contacts

Rody Posthuma
Tech Risk Partner
rody.posthuma@au.ey.com

Hanny Hassan
Tech Risk Partner
hanny.hassan@au.ey.com

Will De Vere Gould
Risk Partner
will.de.vere.gould@au.ey.com

Nikki Bentley
Law Partner
nikki.bentley@au.ey.com

Maree Pallisco
Audit Partner
maree.pallisco@au.ey.com

Walter Poetscher
Oceania Insurance Leader
walter.poetscher@au.ey.com

Douglas Nixon
Oceania Banking and Capital Markets Leader
douglas.nixon@au.ey.com

Rita Da Silva
Oceania Wealth & Asset Management Leader
rita.da.silva@au.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

BMC Agency
GA 134910177

ED None

ey.com