• • • POINT OF VIEW

protiviti®
Global Business Consulting

CPS 230 – APRA’s new standard to improve operational risk and resilience

On 17 July 2023, the Australian Prudential Regulation Authority (APRA) released the final new prudential standard CPS 230 Operational Risk Management, which is mostly aligned to requirements in other jurisdictions, including the United States, the United Kingdom, Hong Kong, and Singapore. The standard aims to reinforce the importance of financial institutions maintaining a clear focus on customer outcomes in their management and oversight of the risk and control environment and service providers, and sets minimum operational resilience requirements that must always be maintained to ensure that any disruptions minimise consumer harm.

Overview

CPS 230 builds on existing standards CPS/SPS /HPS 231 Outsourcing and CPS/SPS 232 Business Continuity Management and will come into effect in July 2025. APRA’s policy and supervision priorities for 2023 also highlight key reforms to strengthen the financial and operational resilience of APRA-regulated entities.

Given the need to comply with the new standard, APRA-regulated institutions need to mobilise projects to diagnose the changes and uplifts required to comply, agree on the end state, and implement change programs.

Below, we set out preliminary measures for designing program end states and effectively implementing associated changes based on our observations from implementations of equivalent operational-resilience programs in other jurisdictions.

Actions financial institutions can take

The following actions are critical for financial institutions to establish an effective change program for CPS 230 that meets regulatory requirements and organisational and service-provider needs and aligns with customer expectations.

Determine critical operations: Adopt a customer-driven focus to identifying critical operations that must be available to meet ongoing customer needs and expectations. Considerations include defining the appropriate number of critical operations required to support customer delivery needs and reestablishing estimated time recovery along with the level of process detail to be captured to minimise harm and ensure that recovery steps have been adequately addressed. Institutions gain the most benefit by adopting a top-down approach to scoping the number of critical operations and actively engaging senior management and the board early in the change program.

Institutions should be objective and mindful of proportionality. The number of critical operations identified will be a central driver of the time and effort required to set tolerance levels, mapping, and testing.

Map and test end-to-end processes for each critical operation: Traditionally, business continuity management plans focus on the recovery of a business function in isolation of the customer needs and priorities. CPS 230’s increased focus on customer outcomes requires institutions to document a clear end-to-end view of the steps and underlying systems, teams and service providers needed to restore critical operations in response to a severe disruption. The requirements can be delivered through effective engagement with senior management, product teams, operations, compliance, risk, technology, cybersecurity, and service providers. An integrated approach to testing and validating existing resilience arrangements (e.g., cyber incident response, business continuity disaster recovery) and tolerance levels are also important to ensure that control weaknesses and gaps are remediated.

Identify and manage service provider exposure and impacts: Service providers are integral and increasingly important to the delivery of products and services to customers, though their level of materiality varies. A service provider may play a material and explicit role in the delivery of a core service that is easily identifiable and manageable or indirect services from fourth-party providers. Institutions need to identify and assess the role each service provider plays in the delivery of customer services and the harm they could cause to customers if compromised. Appropriate processes, controls and governance structures need to be established to manage service-provider relationships, monitor ongoing performance, and align objectives to support operational-resilience objectives. APRA intends to provide transitional arrangements for pre-existing contractual arrangements with service providers, with the requirements in the standard applying from the earlier of the next contract renewal date or 1 July 2026.

Set realistic recovery times to minimise and manage customer harm: Institutions that perform high-quality testing based on the customer- focused process mapping often experience disparities between target customer-harm tolerance levels and the actual time required to recover critical operations. These disparities can be attributed to a lack of understanding or investment in legacy systems, and specified processes inherent to the business environment that have been mapped incorrectly or have not been updated following change. Alternatively, they may be the result of aspirational target-recovery time frames that need to be recalibrated and supported by additional strategies for managing customer expectations to minimise possible harm.

Emphasise board accountability: The board is accountable for operational risk management and is receptive to the concept of operational resilience. It often views resilience as a key strategic driver for its institution's success given the focus on customer experience, particularly during moments of distress.

Actively engaging the board to co-sign a change program is imperative for delivering the program effectively. The board should establish the requirements and expectations for the operational resilience program, including ongoing strategic decisions regarding the role service providers play in the customer journey, the customer harm that may arise and the investment required to restore critical operations, as well as reporting touchpoints that will enable the board to monitor the program.

Acknowledgements

Protiviti Senior Manager Daniel Grazel contributed to this blog.

Contacts

Mark Burgess
Managing Director
Protiviti Australia
+61 411 565 745
mark.burgess@protiviti.com.au

Hirun Tantirigama
Director
Protiviti Australia
+61 423 853 453
hirun.tantirigama@protiviti.com.au

Protiviti (www.protiviti.com/au-en) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk, and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.