WHITEPAPER

CPS 230: How to Drive Operational Resilience and Cyber Preparedness

Regulatory Emphasis on Cyber Resilience

CPS 230, recently released by the Australia Prudential Regulation Authority (APRA), has gained prominence alongside similar standards aimed to promote operational resilience.

Operational resilience refers to an organization's capacity to withstand and adapt to operational disruptions (whether anticipated or unexpected) while ensuring the continuity of critical functions. It is a vital framework for effectively managing risks and safeguarding business continuity despite adversity.

Regulators view cyber resilience as a crucial component of operational resilience. Companies must be well prepared and capable of managing potential challenges resulting from cybercrime effectively.

For example, recently the Security and Exchange Commission (SEC) formalized new disclosure and governance rules requiring public companies to disclose material cyber breaches/incidents within four days of determining the impact. Additionally, public companies are now required to disclose information about their board of directors' oversight of cybersecurity risk. Taken together, this emphasizes the significant importance regulators place on this matter.

Four Key CPS 230 Questions

In a recent webinar, Navigating Operational Resilience: Best Practices and Lessons Learned, SAI360 presented key drivers behind CPS 230 and new findings and market influences on operational resilience. Below are four key questions this webinar addressed:

SAI360
RISK FROM EVERY ANGLE

1. What is the CPS 230 Framework?

CPS 230 is a response to a historical track record of incidents and disruptions that have occurred within the financial sector. Considering these events, Australian regulators have taken proactive measures to address challenges faced by organizations in order to enhance operational resilience.

CPS 230 establishes a comprehensive framework that places significant emphasis on proactive risk identification, robust controls, and transparent reporting. It encompasses a wide range of operational risks, including internal and external fraud, cybersecurity, business disruptions, and regulatory noncompliance.

The final version of CPS 230 was released on July 17, 2023. The new standard will come into effect on July 1, 2025.

APRA has also released a consultation process for CPS 230, a Prudential Practice Guide that will assist organizations with their CPS 230 compliance activities. The consultation period for CPS 230 closes on October 13, 2023.

CPS 230 will apply to a diverse range of entities within the APRA-regulated industry. This includes banks and deposit-taking financial institutions and general insurance and life insurance companies, private health insurers, and superannuation entities. Furthermore, even if a business or firm within a group structure is not directly regulated by APRA, if the head of the group is an APRA-regulated entity, controls and compliance requirements of the new standard will still be applied to those businesses.

2. What are CPS 230's key challenges?

Organizations preparing for CPS 230 implementation face several key challenges. One prominent challenge revolves around accountability, a central theme throughout the standard. APRA expects senior management to be held accountable, with potential financial consequences for non-compliance. Accountability permeates the entire framework, from the Board level to the executive level and individual accountability owners. Merely checking boxes will no longer suffice; organizations must provide evidence that their controls, assurance programs, and adherence to policies and procedures are demonstrable.

Other pillars of CPS 230 include operational risk management, ensuring a robust risk assessment process is ingrained across the organization and encompasses risk types. Additionally, organizations must establish and maintain a comprehensive controls assurance program and possess a thorough understanding of their incident management capabilities, response protocols, and recovery procedures.

Business continuity planning is another critical element of CPS 230 and requires organizations to clearly understand how processes are impacted when there is a disaster, crisis, or other disruption. Organizations need to develop plans that have continuity, including having recovery plans in place and having the necessary resources required for the effective execution of the plans in the case of an event. Organizations are expected to have testing regimes in place to ensure the efficacy of their business continuity plans.

Effective management of service providers is also crucial within the framework. Organizations must have a comprehensive understanding of their vendors and how they impact their services, including material service providers and those who help deliver critical services. Policies and procedures must be well-defined and adhered to.

Furthermore, technology plays a significant role in meeting CPS 230 requirements. APRA has identified technology as an essential component for organizations seeking compliance with the framework. Given the often complex and connected nature of business, its critical processes, the changing risk environment, and the various roles vendors play in supporting their success, it would be almost impossible to find success without a clear and effective technology strategy.

Overall, organizations must address these challenges related to accountability, operational risk management, controls assurance, incident management, business continuity planning, service provider management, policies and procedures, and technology to effectively comply.

3. What is the impact of Medibank's cyber incident on Operational Resilience?

Any operational failure can have profound and enduring consequences for the overall financial stability of local markets.

The emergence of operational resilience as a crucial process for organizations can be attributed to numerous examples highlighting its significance and impact. Medibank is one such example.

In October 2022, Medibank experienced a significant security breach, resulting in the exposure of personal data belonging to all 3.9 million of its customers.

This breach is considered one of Australia's largest personal data security breaches. In response to the incident, Medibank temporarily shut down its customer-facing systems to contain the attack and assess the full extent of the impact. The repercussions of this breach extend beyond Medibank, affecting numerous businesses and individuals.

In part from the financial and reputational damage inflicted upon the organization, APRA announced it will impose an increase in Medibank's capital adequacy requirement to AUD 250 million. APRA's action is a direct response to the vulnerabilities identified in Medibank's cybersecurity and information security environment, discovered during their investigation.

As part of the ongoing investigation, APRA will also conduct a targeted technology review of Medibank, with a specific focus on governance and organizational culture. APRA expects Medibank to ensure personal accountability, including potential impacts on executive remuneration, where appropriate.

Medibank is also subject to an intense investigation and faces scrutiny from Australia's privacy watchdog, the Office of the Australian Information Commissioner, which has partnered with its New Zealand counterpart for the first time. Together, they are examining whether Medibank had adequate security measures in place and investigating the presence of outdated data, some of which dates to 2005.

Such incidents incur significant costs, damage a company's reputation, and lead to regulatory scrutiny and specific actions by governing bodies. APRA's response demonstrates a commitment to taking these matters seriously, and it will heavily regulate weaknesses in controls, assurance frameworks, and information management systems.

4. What are the other key trends to know?

Outside of Australia and CPS 230, there are other key developing international regulations and actions affecting how organizations will need to incorporate operational resilience in the future. One notable example is that SEC has identified Operational Resilience as a priority for the 2023 Exam schedule.

In 2021, the UK Financial Conduct Authority also released Guidelines for Operational Resilience to help firms prevent, adapt, respond to, recover, and learn from operational disruptions. In Europe, the Digital Operational Resilience Act (DORA), has been introduced by the European Banking Authority and is designed to accomplish similar objectives for shoring up operational resilience. These developments are increasing expectations of regulated entities to ensure they are maturing their approach to incident response, business continuity, and third-party risk management.

Regulators are publishing and auditing against these new requirements, guidelines, and standards for good reason. The COVID-19 pandemic illustrated how fragile corporate supply chains were to disruption leaving consumers and investors short of goods and expected financial returns. Natural calamities including the wildfires in California and Australia, hurricanes and flooding across the globe have all forced businesses to shudder, relocate, and find different suppliers. In addition, the growing focus that companies place on digital transformation and harvesting the valuable information they manage is exposing those firms to new risks.

This is evident by the exponential increase in activity and sophistication by cyberthreat actors as illustrated by the rapidly increased number of breaches and ransomware victims.

Digital transformation itself has affected whole industries. In traditional banking, as illustrated by the recent collapse at Silicon Valley Bank, depositors withdrew their funds with ease and speed, triggering a default and bankruptcy that both exposed the banks' poor capital control practices and surfaced a need for changes in regulatory oversight of the industry.

Moreover, Environmental, Social, and Governance (ESG) expectations have corporate executives identifying ways to reduce environmental harm, assess local community impact, and uphold social obligations to employees, stakeholders, and third-party relationships.

While these new regulatory requirements and guidelines bring important investment and focus to the important corporate objective of operational resilience, these new requirements introduce new problems. With the rapid pace of regulatory change in a complex global environment and with thousands of regulatory alerts and changes occurring worldwide every week, organizations will struggle to stay on top of all these requirements on their own.

This complexity extends beyond local regulatory frameworks to include compliance with regulations in various operating environments, such as the General Data Protection Regulation (GDPR) for handling EU (European Union) residents' information. Many large organizations still operate in silos and rely on manual processes for information and communication. This only highlights the need for more integrated, efficient approaches.

FINAL THOUGHTS

Operational resilience is not just important for financial institutions. Regulators of many other industries, especially those classified as “Critical Infrastructure”, have long recognized the importance of operational resilience. While these industries, like energy, pharmaceuticals, and government, may have existing requirements in place, they are also impacted by the increased velocity and magnitude of these and other industry-specific threats. In response, they are updating requirements, guidance, and audit frequency and scope.

For any organization looking to improve and enhance its operational resilience, APRA’s CPS 230 is another resource to improve operational resilience and competitiveness in the face of disruptions and market competition.

For more information, click here to watch our full webinar: Navigating Operational Resilience: Best Practices and Lessons Learned.

Interested in learning how SAI360’s prebuilt module can help you monitor, manage, and prevent organizational disruptions?

Request a demo.

Our unified approach to risk sets us apart

Today’s complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

154253 0324